EXHIBIT 2

Lesley Weaver (Cal. Bar No.191305)
Angelica M. Ornelas (Cal. Bar No. 285929)
Joshua D. Samra (Cal. Bar No. 313050)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, CA 994607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
aornelas@bfalaw.com
jsamra@bfalaw.com

Mitchell M. Breit (*pro hac vice* to be sought)
Jason 'Jay' Barnes (*pro hac vice* to be sought)
An Truong (*pro hac vice* to be sought)
Eric Johnson (*pro hac vice* to be sought)
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

Laurence D. King (Cal. Bar No. 206423)
Mario Choi (Cal. Bar No. 243409)
KAPLAN FOX & KILSHEIMER LLP
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com
mchoi@kaplanfox.com

David A. Straite (*pro hac vice* to be sought)
Aaron L. Schwartz (*pro hac vice* to be sought)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue
New York, NY 10022
Tel.: (212) 687-1980
Fax: (212) 687-7715
dstraite@kaplanfox.com
aschwartz@kaplanfox.com

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, ELAINE CRESPO, HADIYAH JACKSON and CLAUDIA KINDLER, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

No. ____________________________

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

PUBLIC REDACTED VERSION WITH PLAINTIFFS' SENSITIVE PERSONAL INFORMATION PROVISIONALLY REDACTED PENDING MOTION TO SEAL

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd.)

TABLE OF EXHIBITS

EX.	DOCUMENT DESCRIPTION
1	Chart of Documents Constituting the Relevant Contract by Date
2	Google Terms of Service dated April 14, 2014
3	Google Terms of Service dated Oct. 25, 2017
4	Google Terms of Service dated March 31, 2020
5	Chrome Terms of Service dated Aug. 12, 2010
6	Google Chrome and Chrome OS Additional Terms of Service dated March 31, 2020
7	Google Privacy Policy dated June 28, 2016
8	Google Privacy Policy dated Aug. 29, 2016
9	Google Privacy Policy dated March 1, 2017
10	Google Privacy Policy dated April 17, 2017
11	Google Privacy Policy dated Oct. 2, 2017
12	Google Privacy Policy dated Dec. 18, 2017
13	Google Privacy Policy dated May 25, 2018
14	Google Privacy Policy dated Jan. 22, 2019
15	Google Privacy Policy dated Oct. 15, 2019
16	Google Privacy Policy dated Dec. 19, 2019
17	Chrome Privacy Notice dated June 21, 2016
18	Chrome Privacy Notice dated August 30, 2016
19	Chrome Privacy Notice dated Oct. 11, 2016
20	Chrome Privacy Notice dated Nov. 30, 2016
21	Chrome Privacy Notice dated Jan. 24, 2017
22	Chrome Privacy Notice dated March 7, 2017
23	Chrome Privacy Notice dated April 25, 2017

TABLE OF EXHIBITS

EX.	DOCUMENT DESCRIPTION
24	Chrome Privacy Notice dated March 6, 2018
25	Chrome Privacy Notice dated Sept. 24, 2018
26	Chrome Privacy Notice dated Oct. 24, 2018
27	Chrome Privacy Notice dated Dec. 4, 2018
28	Chrome Privacy Notice dated Jan. 30, 2019
29	Chrome Privacy Notice dated Mar. 12, 2019
30	Chrome Privacy Notice dated Oct. 31, 2019
31	Chrome Privacy Notice dated Dec. 10, 2019
32	Chrome Privacy Notice dated March 17, 2020
33	Chrome Privacy Notice dated May 20, 2020

I. INTRODUCTION

1. This is a nationwide data privacy class action brought by and on behalf of Google Chrome users who chose not to "Sync" their browsers with their Google accounts while browsing the web ("Un-Synched Chrome Users") from July 27, 2016 to the present (the "Relevant Period").

2. Google expressly promises Chrome users that they "don't need to provide any personal information to use Chrome" and that "[t]he personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync[.]"

3. Despite these express and binding promises, Google intentionally and unlawfully causes Chrome to record and send users' personal information to Google ***regardless of whether a user elects to Sync or even has a Google account.***

4. Examples of personal data improperly created and sent to Google by Chrome include:

a. IP addresses linked to user agents;

b. Unique, persistent cookie identifiers including the Client ID;

c. Unique browser identifiers called X-Client Data Headers; and

d. Browsing history.

5. This Complaint provides specific examples of the personal data flow that Chrome sent from Plaintiffs' devices as they used Chrome while not Synched, demonstrating that Chrome secretly sends personal information to Google even when a Chrome user does not Sync.

6. Google's contract with Chrome users designates California law, and consistent with California law, defines "Personal Information" as "information that you provide to us which personally identifies you . . . ***or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account***."

7. Each category of data identified above is "personal information" because it either personally identifies the user or can be reasonably linked to such information. Furthermore, Google affirmatively discloses that it associates data gathered from Chrome with users. Google has therefore breached its contract with Un-Synched Chrome Users.

8. The improperly collected web browsing history also consists of electronic communications that contain content protected by California and federal wiretap laws. Google collects the content contemporaneously with the communications; Google does not obtain consent from Un-Synched Chrome Users to intercept these communications; and Google is not a party to them. Google is thus violating the federal Electronic Communications Privacy Act and analogue California statutes.

9. Google's actions are a serious violation of user privacy. Google tracking code is found on websites accounting for more than half of all internet traffic and Chrome is the dominant web browser (used on a majority of desktop computers in the United States), giving Google unprecedented power to surveil the lives of more than half of the online country in real time. And because some of Google's third-party tracking cookies are disguised as first-party cookies to facilitate cookie synching, Google is misrepresenting its privacy practices in ways that have been successfully challenged by the FTC in the past.[1]

10. Google's extensive network of affiliates—Google Sites, Google Apps, Google Account, Google Drive, Google AdWords—as well as its business partnerships means that sharing information with Google feeds it into a massive interconnected database of surveillance material. Google's surveillance of the Plaintiffs and other Un-Synched Chrome Users directly contradicts its promises to honor users' choice not to share data. This is a serious and irreversible invasion of privacy that is invisible to Google users.

11. Google's actions also constitute rank theft. Plaintiffs' PI is a form of property recognized under California law and has economic value in the marketplace. Taking Plaintiffs' PI from their computers without consent is larceny; any profits earned on the PI are unjustly earned at the expense of Plaintiffs and must be disgorged. Had Google been transparent about its level of surveillance, user engagement—a key metric for Google's sales—would have decreased.

12. Google's actions also constitute unlawful computer intrusion under California and federal law. Google introduced computer code into Plaintiffs' computers and caused damage

[1] *United States v. Google, Inc.*, 12-cv-4177-SI (N.D. Cal.), complaint dated Aug. 8, 2012, at ¶ 46-47.

without authorization by turning the computers into surveillance machines that reported Plaintiffs' personal information, including private web browsing, to Google, in real time.

13. Plaintiffs and the other Un-Synched Chrome Users have suffered privacy harm and economic harm as a result of Google's wrongful acts. Plaintiffs therefore bring contract, statutory, common law and equitable claims against Google for money damages, restitution, disgorgement, punitive damages and injunctive relief.

II. JURISDICTION AND VENUE

A. Personal Jurisdiction

14. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District. Google also concedes personal jurisdiction in the current and prior general Google Terms of Service. *See* Exhibits 2 through 4.

B. Subject Matter Jurisdiction

15. This Court has subject matter jurisdiction over the federal claims in this action, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act"), the Stored Communication Act, 18 U.S.C. § 2701 ("SCA"), the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") and request for Declaratory Relief under 18 U.S.C. § 2201, pursuant to 28 U.S.C. § 1331.

16. This Court also has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than California or Delaware.

17. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

C. Venue

18. Venue is proper in this District because the Defendant is headquartered in this District. In addition, in the current Google general Terms of Service and prior versions, Google purports to bind Plaintiffs to bring disputes in this District. *See* Exhibits 2 through 4.

III. THE INTRADISTRICT ASSIGNMENT

19. Assignment of this case to the San Jose Division is proper pursuant to Civil Local Rule 3-2(c)(e) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Santa Clara County, California.

IV. PARTIES

20. Plaintiff Patrick Calhoun is an adult domiciled in Florida. Plaintiff has used the Chrome browser on his personal laptop for numerous activities, including exchanging communications with state government agencies [redacted]. Plaintiff has also routinely used the Chrome browser to exchange communications about news, politics, and more. Plaintiff has not enabled Sync with his Google accounts on his personal laptop and never consented to Chrome sharing his Personal Information, including the contents of his Internet communications, with Google. Despite his lack of consent and expressly promising otherwise, Chrome shared Calhoun's personal information with Google, including the content of his communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again once Google stops tracking un-synched users.

21. Plaintiff Elaine Crespo is an adult domiciled in Florida. Plaintiff has used the Chrome browser on her personal laptop for numerous activities, including exchanging communications relating to banking, her children's education, and for her employment. Plaintiff has not enabled Sync with her Google accounts on her personal laptop and never consented to Chrome share her personal information, including the contents of her Internet communications, with Google. Despite her lack of consent and expressly promising otherwise, Chrome shared Crespo's personal information with Google, including the contents of her communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again once Google stops tracking un-synched users.

22. Plaintiff Hadiyah Jackson is an adult domiciled in Pennsylvania. Plaintiff and her family have used the Chrome browser on her personal laptop for numerous activities, including exchanging communications with state government agencies regarding an [redacted] [redacted] Plaintiff has not enabled Sync with her Google accounts on her personal

laptops and never consented to Chrome sharing her Personal Information, including the contents of her Internet communications, with Google. Despite her lack of consent and expressly promising otherwise, Chrome shared Jackson's personal information with Google, including the content of her communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again once Google stops tracking un-synched users.

23. Plaintiff Claudia Kindler is an adult domiciled in California. Plaintiff has used the Chrome browser on her personal laptop for numerous activities, including exchanging communications with her banks, healthcare providers, and continuing education providers for her employment. Kindler has also routinely used the Chrome browser to exchange communications about politics and more. Plaintiff has not enabled Sync with her Google accounts on her personal laptops and never consented to Chrome sharing her Personal Information, including the contents of her Internet communications, with Google. Despite her lack of consent and expressly promising otherwise, Chrome shared Kindler's personal information with Google, including the content of her communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again once Google stops tracking un-synched users.

24. Google LLC ("Google") is a Delaware Limited Liability Company based at 1600 Amphitheatre Way, Mountain View, California, whose memberships interests are entirely held by its parent holding company, Alphabet, Inc. ("Alphabet"), headquartered at the same address. Alphabet trades under the stock trading symbols GOOG and GOOGL. Alphabet generates revenues primarily by delivered targeted online advertising through the Google LLC subsidiary. All operations relevant to this complaint are run by Google LLC.

25. In this Complaint, "Google" refers to Google LLC unless otherwise specified

V. FACTUAL ALLEGATIONS

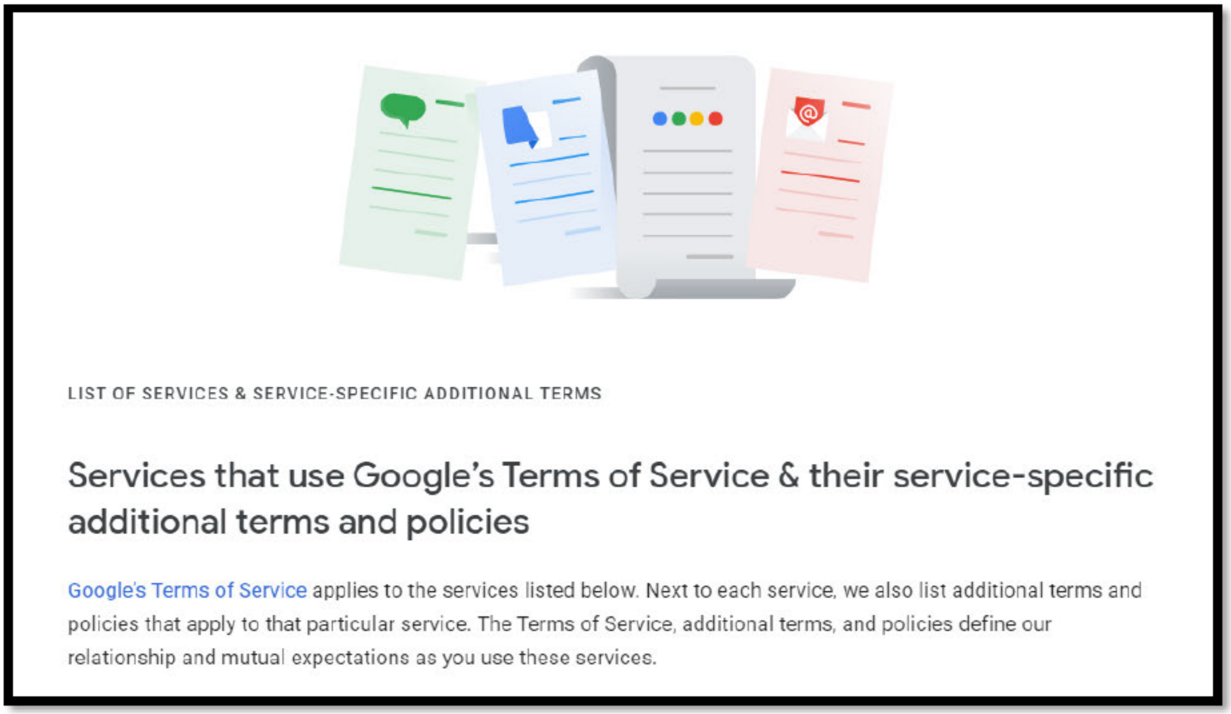
A. Contract Formation

26. The current contract governing the relationship between Google and Chrome with respect to Chrome consists of three documents: the Google general Terms of Service dated March 31, 2020 (Exhibit 4) ("General TOS"); the Google Chrome and Chrome OS Additional

Terms of Service dated March 31, 2020 (Exhibit 6) ("Chrome TOS"); and the Chrome Privacy Notice dated May 20, 2020 (Exhibit 33) ("Chrome Privacy Notice").[2]

27. These documents are revised frequently, see chart in Exhibit 1, but the core contract terms relevant to this Action are the same throughout the Relevant Period.

28. The General TOS incorporates by reference and hyperlinks to "service-specific additional terms and policies" as illustrated below and in Exhibit 4. The General TOS provides that certain identified services are governed by the General TOS as well as "additional terms and policies that apply to that particular service." It continues, "[t]he Terms of Service, ***additional terms and policies*** define our relationship and mutual expectations as you use these services":



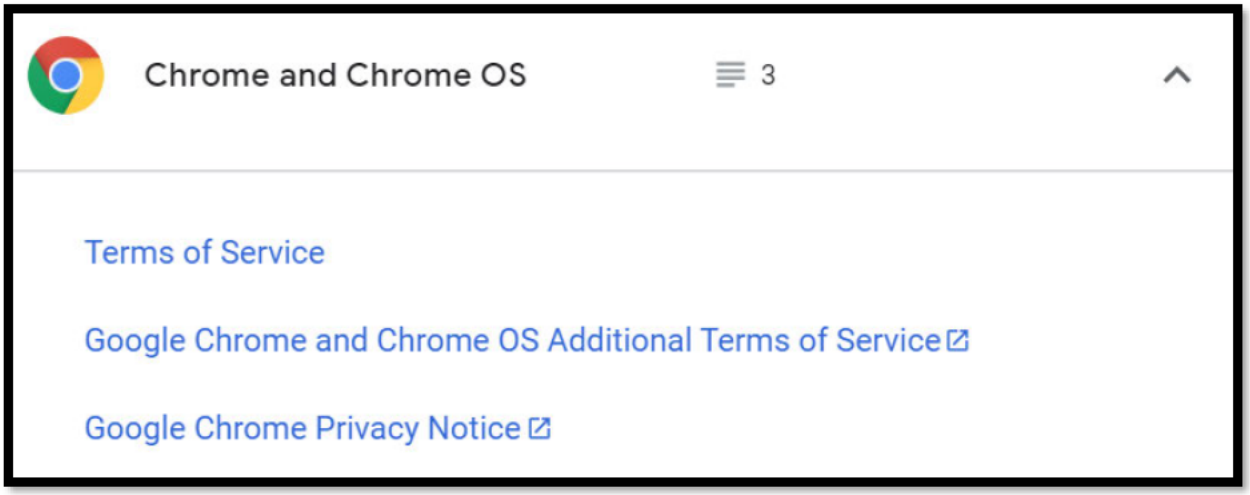
LIST OF SERVICES & SERVICE-SPECIFIC ADDITIONAL TERMS

Services that use Google's Terms of Service & their service-specific additional terms and policies

Google's Terms of Service applies to the services listed below. Next to each service, we also list additional terms and policies that apply to that particular service. The Terms of Service, additional terms, and policies define our relationship and mutual expectations as you use these services.

[2] Prior to March 31, 2020, the contract also included a fourth document, the Google general Privacy Policy (Exhibits 7 through 16).

29. The General TOS then identifies Chrome as a "service" and identifies (and hyperlinks to) three documents that govern the use of Chrome and together constitute the contract:


Chrome and Chrome OS

Terms of Service

Google Chrome and Chrome OS Additional Terms of Service

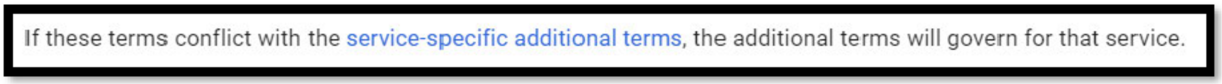
Google Chrome Privacy Notice

30. The General TOS contains 15 separate references and links to the "service-specific additional terms and policies." Every time this term is referenced, a hyperlink is included that incorporates and links users to the "List of services & service-specific additional terms."

31. Prior to March 31, 2020, the Chrome TOS itself also expressly incorporated the Chrome Privacy Notice as a part of the contract. The Chrome TOS dated Aug. 12, 2010 states that users' "agreement with Google" includes "the terms set forth" in the General TOS as well as "Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the Services." *See* Ex. 5.

32. The Chrome TOS further states that "[f]or more information about Google's data protection practices, please read Google's privacy policy at http://www.google.com/privacy.html and at https://www.google.com/intl/en/chrome/privacy/." These two URLs link to the web pages where the Google Privacy Policy and the Chrome Privacy Notice were publicly available.

33. Finally, the General TOS specifies that "service-specific additional terms" govern where there is a conflict with the General TOS:


If these terms conflict with the service-specific additional terms, the additional terms will govern for that service.

34. At all times during the Relevant Period, therefore, the Chrome Privacy Notice was a part of the contract between Plaintiffs and Google and supersedes any conflicting term in the General TOS.

B. Relevant Contract Terms

35. The Chrome Privacy Notice represents that it is the place where users can "Learn to control the information that's collected, stored, and shared when you use the Google Chrome browser[.]" *See* Ex. 33.

36. In the Chrome Privacy Notice, Google promised that Chrome would not send any Personal Information to Google unless the Chrome User affirmatively chose to Sync the browser with his or her Google Account.

37. Specifically, from June 2016 to present, all versions of the Chrome Privacy Notice have promised that "You don't need to provide any personal information to use Chrome." *See* Exs. 17-33.

38. In addition, all versions of the Chrome Privacy Notice have promised that Chrome will not send Personal Information to Google unless the Chrome user chooses to Sync the browser with his or her Google account:

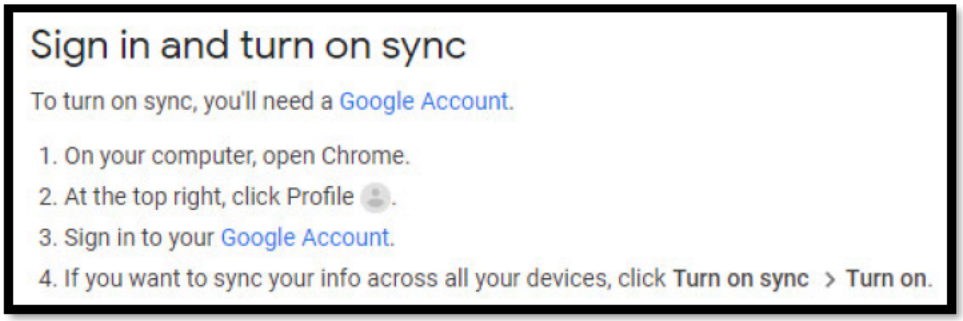
a. From January 30, 2019 to the present, Google promises that "the personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync." *See* Exs. 28-33.

b. From September 24, 2018 to January 30, 2019, Google promised that "the personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on Chrome sync." *See* Exs. 25-27.

c. Prior to September 24, 2018, the Chrome Privacy Notice promised "The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by signing in to Chrome. Signing in enables Chrome's synchronization feature." *See* Exs. 17-24.

39. The Chrome Privacy Notice has always promised that Sync will only be enabled by your choice to take an affirmative act. Synching has never been a default setting during the Relevant Period. For example, from September 24, 2018 to present, a Chrome user had to take the follow affirmative steps to enable Sync:

a. On a desktop,[3] the user can enable Sync by taking "open[ing] Chrome, clicking the "Profile" icon at the top right, signing in to the user's "Google Account," clicking "Turn on sync" and then "Turn on." An example is shown here:



Sign in and turn on sync

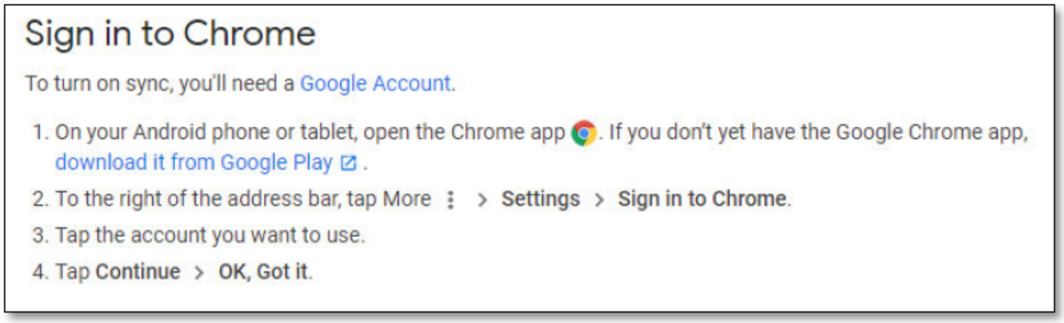
To turn on sync, you'll need a Google Account.

1. On your computer, open Chrome.
2. At the top right, click Profile .
3. Sign in to your Google Account.
4. If you want to sync your info across all your devices, click **Turn on sync** > **Turn on**.

b. On a mobile device, a user downloads the Chrome app, clicks the "…" to the right of the address bar, clicks "Settings," then clicks "Sign in to Chrome," then "Tap the account [the user] want[s] to use," tap "Continue," and then tap "OK, Got it." An example of these steps for Android users is shown below:[4]

[3] *Turning sync on and off in Chrome*, Google Chrome Help, https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DDesktop&oco=1 (last visited July 19, 2020).

[4] *Turn sync on and off in Chrome*, Google Chrome Help https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DAndroid&oco=1 (last visited July 19, 2020).

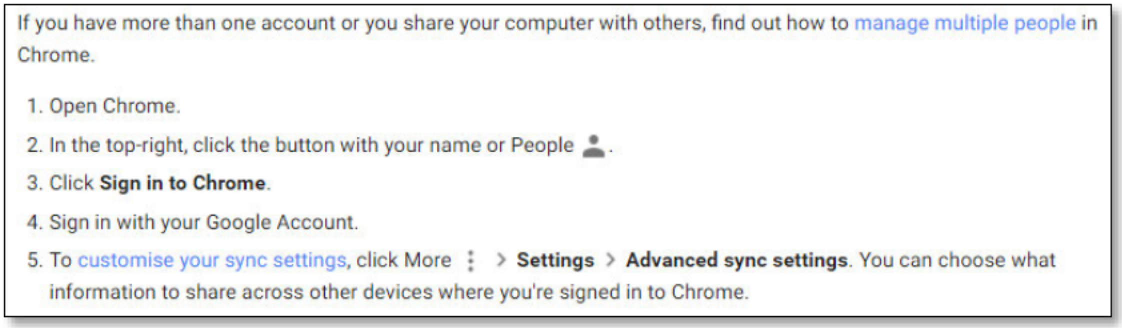


Sign in to Chrome

To turn on sync, you'll need a Google Account.

1. On your Android phone or tablet, open the Chrome app. If you don't yet have the Google Chrome app, download it from Google Play.
2. To the right of the address bar, tap More ⋮ > **Settings** > **Sign in to Chrome**.
3. Tap the account you want to use.
4. Tap **Continue** > **OK, Got it**.

40. Prior to September 24, 2018, the process was different but still required at least four affirmative steps to enable Chrome synchronization through the Chrome sign-in feature.[5]



If you have more than one account or you share your computer with others, find out how to manage multiple people in Chrome.

1. Open Chrome.
2. In the top-right, click the button with your name or People 👤.
3. Click **Sign in to Chrome**.
4. Sign in with your Google Account.
5. To customise your sync settings, click More ⋮ > **Settings** > **Advanced sync settings**. You can choose what information to share across other devices where you're signed in to Chrome.

41. On mobile devices, users had to take similar steps to enable Chrome.[6]

C. Google Improperly Collects Personal Information from Un-Synched Chrome Users Without Consent and in Breach of Contract

1. Definition of Personal Information

42. The contract designates California law as the governing law.

43. California law defines "Personal Information" as, and it is used in this Complaint to mean: "information that identifies, relates to, describes, ***is reasonably capable of being associated with***, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

[5] Sign in to Chrome, Chrome Help, https://web.archive.org/web/20170411045120 /https://support.google.com/chrome/answer/185277 (archived on Apr. 11, 2017).

[6] *See e.g.*, Travis Boylss, *How to Sync Bookmarks on Chrome on iPhone or iPad*, WikiHow (Dec. 24, 2017), https://www.wikihow.tech/Sync-Bookmarks-on-Chrome-on-iPhone-or-iPad.

Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

a. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

b. Any categories of personal information described in subdivision (e) of Section 1798.80.

c. Characteristics of protected classifications under California or federal law;

d. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

e. Biometric information;

f. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;

g. Geolocation data;

h. Audio, electronic, visual, thermal, olfactory, or similar information;

i. Professional or employment-related information;

j. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232(g); 34 C.F.R. Part 99);

k. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

44. The Google general Privacy Policy also expressly tracks the California statutory definition of "personal information," defining it as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, ***or other data that can be reasonably linked to such information by Google***, such as information we associate with your Google Account." *See* Ex. 16 (emphasis added).

45. The following data qualifies as personal information when Google code instructs the Google Chrome browser to report it to Google:

a. IP addresses linked to user agent;

b. Session and Persistent cookie identifiers;

c. X-client-data headers; and

e. Browsing history and information regarding a consumer's interaction with an Internet website.

46. Google is reasonably capable of linking IP addresses (including those linked to user agent), persistent cookie identifiers, X-client-data headers, and web browsing history and information regarding a consumer's interaction with an Internet website, and, in fact, does link such information with individual consumers and their devices.

2. An IP Address + User Agent Is Personal Information

47. An IP address is a number that identifies a computer connected to the Internet.

48. IP addresses are used to identify and route communications on the Internet.

49. An IP address is not the same thing as a URL.

50. IP addresses of individual Internet users are used by Internet service providers, websites, and tracking companies to facilitate and track Internet communications.

51. Google tracks IP addresses associated with specific Internet users.

52. Google is capable of and does in fact associate specific users with specific IP addresses. For example, when a user signs into a Gmail account, Google associates the personal information connected with that email account to the IP address in question.

53. Even if a specific IP address is shared by multiple devices on a single network, Google is capable of and does, in fact, associate specific users with specific IP addresses. Google does so through its use of other identifiers tied to an IP address, including User-Agent, which is a list of properties identifying a device within a network.

54. Because Google collects the IP Address and user agent information together, Google can identify a user's individual device even if more than one device shares the same IP Address.

3. Persistent Cookies Are Personal Information

55. A cookie is a small text file that a web-server can place on a person's web browser and computing device when that person's web browser interacts with the website server.

56. Cookies can perform different functions. Eventually, some cookies were designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

57. Cookies are designed to and, in fact, do operate as a means of identification for Internet users.

58. In general, cookies are categorized by (1) duration and (2) party.

59. There are two types of cookies classified by duration:

a. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie during a single communication session. The user's web browser deletes session cookies when the user closes the browser.

b. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's Internet communications for years and over dozens, hundreds, or thousands of websites. Persistent cookies are sometimes called "tracking cookies."

60. Cookies are also classified by the party that uses the collected data:

a. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. For example, Google uses cookies on users' browsers when users' directly visit Google properties such as Gmail. First-party cookies can be helpful to the user, server, and/or website to assist with security, log-in, and functionality.

b. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same Gmail user might also have cookies on their Chrome browser that are set by Google's other services such as Google Ads or Google Doubleclick. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

61. Google uses several cookies to identify specific Internet users and their devices, including the following:

SID **HSID**	These cookies contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time. They are unique and persistent on a user's device for two years or more.
_Secure-SSID **_Secure-HSID**	These cookies are "secure" cookies that Google sets and accesses when a user signs into a Gmail account and does not formally log-off even after the user has left the Gmail website. They are unique and persistent on a user's device for six months or more.
NID	The NID cookie contains a unique ID Google uses to remember user preferences and other information, including, for example, how many search results they wish to have shown per page and whether they have Google's SafeSearch filter turned on. NID is also used to help customize ads on Google properties, like Google search. NID is unique and persistent on a user's device for two years or more.
SSID **APISID** **SAPISID**	These cookies are unique and persistent on a user's device for two years or more. Google does not publicly state their purpose.
_Secure-3PSID **_Secure-APISID** **Secure-3PAPISID**	These cookies are "secure" cookies that Google sets and accesses when a user signs into a Gmail account and does not formally log-off even after the user has left the Gmail website.
IDE	Google uses the IDE cookie for advertising. It is unique and persistent on a user's device for two years or more.
DSID	Google also uses the DSID cookie for advertising. It is unique and persistent on a user's device for two years or more.

62. Google also engages in a controversial practice known as "cookie synching" which further allows Google to associate cookies with specific individuals. With cookie synching, first-

party cookies are set by websites with which users are directly interacting, but then those first-party websites also pass that cookie values along to Google Analytics, where Google takes the personal information it has about the user's particular browser and links the Google Analytics first-party cookie information to Google's own third-party cookies and the user's browsing.

63. Based on an Internet security policy known as the same-origin policy, web-browsers are supposed to prevent different entities from accessing each other's cookies. For example, at the San Jose Mercury News website, Google would be prevented from accessing the new site's "first-party" cookie values. And vice-versa, the San Jose Mercury News would be prevented from accessing Google.com's third-party cookie values.

64. However, Javascript source code running on a webpage can bypass the same origin policy protections by sending a putative 'first-party' cookie value in a tracking pixel to a third-party entity. This technique is known in the Internet advertising business as "cookie synching."

65. Cookie synching allows cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is complete, the two websites exchange information that they have collected and hold about a user, further making these cookies "Personal Information."

66. The Google cookie-synching cookie is called "*cid*," which is short for the "Client ID" that Google assigns to a specific user. As Google admits in its Google Analytics documentation for web-developers, the *cid* cookie is personal information:

> In order for Google Analytics to determine that two distinct hits belong to the same user, a unique identifier, associated with that particular user, must be sent with each hit. The analytics.js library accomplishes this via the Client ID field, a unique, randomly generated string that gets stored in the browser's cookies, ***so subsequent visits to the same site can be associated with the same user***.[7]

67. Chrome shares the Client ID value with Google regardless of a user's Sync status or log-in status with Google Ads, Google Doubleclick, and Google Analytics. Even worse, Chrome shares Google's *cid* cookie value with Google even when third-party cookies are blocked.

[7] https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id.

Disguising third-party tracking cookies as first-party cookies is a deceptive privacy practice already successfully challenged by the FTC when Google attempted it in 2011. *United States v. Google, Inc*., 12-cv-4177-SI (N.D. Cal.), complaint dated Aug. 8, 2012, at ¶ 46-47.

68. In addition to sending Google the “CID” cookie value, Chrome also sends cookie-synched values for Google cookies named *_gads ID*, *_gcl_au/auiddc*, and *_gid* to Google.

4. X-Client Data Headers Are Personal Information

69. The x-client-data header is an identifier that when combined with IP address and user-agent, uniquely identifies every individual download version of the Chrome browser.

70. The x-client-data identifier is sent from Chrome to Google every time users exchange an Internet communication, including when users log-in to their specific Google accounts, use Google services such as Google search or Google maps, and when Chrome users are neither signed-in to their Google accounts nor using any Google service.

71. Chrome has created and sent the x-client-data identifier to Google with every communication users exchange since at least March 6, 2018.

72. The x-client-identifier is not disclosed in any term of service or privacy policy operative at any time.

73. It is also not hyperlinked to any of these policies and the average, reasonable Chrome user had no reason to know of its existence.

74. Google first publicly admitted to the existence of the x-client-data identifier to the tech community in a document called the Chrome Privacy White Paper, published on March 6, 2018. The White Paper assisted developers on the “read” side—or surveillance side—with developing products that could extract this information and further pair it with existing data.

75. The White Paper is authored by Google and makes several admissions relevant to this action, as well as furthering the impression that Chrome was not sending personal information to Google in violation of its express promises.

76. The White Paper begins by stating, “This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine).”

77. Despite claiming the it would “describe[] the features in Chrome that communicate with Google[,]” the White Paper does not disclose that Chrome sends users’ personal information to Google regardless of whether users are logged-in to their Google Sync account or not.

78. Initially, the White Paper falsely represented that the x-client data identifier, which it called a “Chrome-Variations header” did “not contain any personally identifiable information and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation.”[8]

79. However, on September 24, 2018, researcher and technologist Vincent Toubiana with ARCEP (a French Telecom regulator), who runs the blog www.unsearcher.org, took notice of X-client-data. What he learned alarmed him:

> **“The x-client-data header**
>
> This is probably the most problematic header and I did not see it mention anywhere else than in the whitepaper. ***Most users are not aware of it but this header is sent with every request sent to Google services*** (and only Google services) to do A/B testing. Google services include most Google domains, including Doubleclick. Even when Google is a third party, the header is sent. Because it’s a header and not a cookie, it is sent even when you block cookies.
>
> . . . .
>
> ***So not only does this header may* [sic] *have some privacy implications, it makes the browser not neutral as it gives more data to Google services.***
>
> …
>
> **Conclusion**
>
> . . . by using custom headers, Google is less and less dependent on third party cookies. *I would not be surprised if Chrome started to block third party cookies*. Actually this may be in Google financial interest to do that.[9]

[8] https://web.archive.org/web/20180505082442/https://www.google.com/chrome/privacy/whitepaper.html

[9] https://unsearcher.org/more-on-chrome-updates-and-headers

80. On January 14, 2020, Google announced that Chrome would be phasing out the use of third-party cookies over two years. Google cynically claimed that its decision was driven by the fact that "[u]sers are demanding greater privacy—including transparency, choice, and control over how their data is used."[10] Left unsaid was the fact that ***Chrome's x-client header can now uniquely identify a majority of web-browsers in the United States, and Google does not need tracking cookies anymore***. Now that Google controls both the online ad market and the browser market simultaneously, blocking third-party cookies simply blocks competing trackers, while Google has a method to continue back-door tracking through the unique browser identifier created and disclosed by its browser without any notification to users.

81. In addition to uniquely identifying Plaintiffs' browsers, Google also uses the x-client-identifier to track them across other Google services. For example, on February 4, 2020, Arnaud Granal, the developer of the Kiwi Browser (a Chromium-based alternative browser for Android) discovered and disclosed that x-client-data is "a unique ID to track a specific Chrome instance across all Google properties," including, in his example, YouTube and Doubleclick.[11]

82. Similarly, Kyle Bradshaw at www.9to5google.com explained the x-client-data identifier "is sent to those Google servers regardless of whether you're logged in with your Google Account or not, which could theoretically tie your logged-out browsing back to your Google Account."[12]

83. Bradshaw further explained, "Putting it all together, the accusation being leveled against Google by the tech community is that the company is making it harder for competing ad networks and other third-parties to track your browsing while their own purported tracking method is able to continue uninhibited." Regardless of the impact on competitors, the impact on Plaintiffs and the Class is significant—they cannot escape this new and even more secretive form of surveillance.

[10] https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[11] https://github.com/w3ctag/design-reviews/issues/467#issuecomment-581944600

[12] https://9to5google.com/2020/02/06/google-chrome-x-client-data-tracking/

84. Following the revelations above, Google quietly amended its White Paper to remove its false representations about the x-client header. For example, on March 12, 2020, in an article called "Google Backpedals on Claim that X-Client-Data Doesn't Contain PI Information," it was reported by VPN Overview:

> Originally the information about the X-Client-Data header in the whitepaper was as follows: "A list of field trials that are currently active on your installation of Chrome will be included in all requests sent to Google. This Chrome variations header (X-Client-Data) will not contain any personally identifiable information, and will only describe the state of the installation of Chrome itself, including active variations, as well as server-side experiments that may affect the installation." ***In the latest version of the whitepaper, the text stating that the X-Client-Data header doesn't contain any PI information has been removed***.[13]

85. VPN Overview further explained:

> The fact that Google may be tracking users through the X-Client-Data header, is in itself of concern. However, it is not the most important issue here. Google probably has other means for tracking users. ***Of greater concern is the fact that Google did not disclose what it was using the header for. Google is tracking users without their knowledge, which is a violation of users' privacy. Furthermore, the original description of the header's use was incredibly inaccurate and likely to have been in breach of legal compliance requirements.***

86. As of the date of filing, Google still has not fixed the Chrome Privacy Notice, the Google general Terms of Use, or the Google Privacy Policy to accurately disclose the X-Client-Data identifier and its uses.

5. Browsing History is Personal Information

87. Browsing history consists of a record of a communication or communications that a user exchanges on the Internet and includes both the content of the communication or communications and data associated with it, such as the time of the communication or communications.

88. California law defines "personal information" to include browsing history, specifically, "Internet or other electronic network activity information, including, but not limited

[13] https://vpnoverview.com/news/google-backpedals-on-claim-that-x-client-data-doesnt-contain-pi-information/

to, browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement.” Cal. Civ. Code § 1798.140(o)(1)(F).

89. Google also defines “personal information” to include browsing history in the Chrome Privacy Notice.

D. Chrome’s Promise Not To Share PI With Google if Not Synched Was Intended To Encourage, Not Diminish, User Engagement

90. Google’s motivation to breach its privacy promises to Un-Synched Chrome Users was to increase user engagement and increase revenue for Google. Higher user engagement means more revenue in that moment for Google, and also more data about the users that can lead to more revenue. By promising more privacy, Google induces more private sharing, which is a more profitable kind of user engagement.

91. “User engagement” is the degree to which users find products, services and processes interesting or useful. It is typically measured by time spent interacting with products and user satisfaction with that time spent. Engagement can be measured by a variety or combination of activities such as downloads, clicks, interactions, shares, and more.

92. Examples of “engagement” data include:

a. For social or traditional media sites: daily usage, views, time on page, pages per visit, ad clicks, searches, comments, or shares;

b. For streaming music apps: daily usage, time spent in app, songs listened to, playlists created, friends added;

c. For an e-commerce store: monthly usage, adding items to cart;

d. For a personal finance app: weekly usage, sync bank accounts, create a budget, enable notifications, view dashboard; and

e. Enterprise software: Monthly usage, create reports, share reports, invite users.

93. Examples of specific metrics used by online entities to track this engagement include daily active users (DAU), cost-per-acquisition, and ROI. The relative value of these metrics varies by business. For example, high engagement via views or clicks might be good for a news site but

not for an insurance app, where more usage might suggest that a user is about to file a claim. Higher engagement leads to higher profits when additional activity leads to purchases, signups, subscriptions, ad views, or clicks.

94. Product and marketing teams typically measure user engagement to understand the factors that contribute to higher engagement and use product analytics measure what features affect user behavior. Product analytics and active user engagement data important selling points to advertisers and those who will pay to influences user behavior, whether that is to purchase something, vote or take some other action.

95. By inducing more personal and more active engagement, Google can therefore increase its profitability. Because this is a revenue-generating exercise, analytics teams at Google are incentivized to engage in detailed analysis of both how to stimulate more engagement, and also the value of each kind of engagement and the data that it generates. Put differently, specific user engagement are assigned economic value.

96. By analyzing user flow—where users spend time, how they interact with others, when they disengage with a site or app or maybe interested in paying more to upgrade—Google can learn valuable insights into how to influence users' choices and how to target them for Google's partners. User flow is analyzed by using precisely the metrics at issue in this action.

97. Indeed, Google was a pioneer in this field, and Google products help developers create Engagement Scores for users.[14] In June 2011 Google acquired PostRank, specifically because PostRank had an effective tool for measuring user engagement. According to a Google spokesperson at that time, Google is "always looking for new ways to measure and analyze data," and PostRank would help "make this data more actionable and accountable [through] an innovative approach to measuring web engagement [that can] help us improve our products for our users and advertisers.[15]

[14] https://www.chromium.org/developers/design-documents/site-engagement

[15] https://techcrunch.com/2011/06/03/google-acquires-postrank-an-analytics-service-for-the-social-web/

98. As applied here, the data that Chrome has sent to Google in violation of its promises not to do so is integral to the calculation of users' engagement scores. It can also be tied to specific profitability.

99. The most powerful of all of these may be the x-client-referrer header, described above. Because it is all-pervasive and impossible to remove from users' activity, the richness of the data Google collects has higher value than disconnected data points of less robust detail.

100. By targeting advertising at users who have a higher amount of "tracked" engagement, Google can increase the profits they make from gathering that data.

101. An "untracked" user may only be shown generic ads. Such ads, in turn, tend to yield a lower engagement rate and therefore generate less profit for Google. A "tracked" user's browsing, in contrast, yields greater data for Google to target and is also a more lucrative target in its own right. The more active a user is, the more vulnerable to targeting she is, and more valuable as well.

102. In addition, promising a user that she is free from tracking induces a different set of expectations and also a different kind of engagement. Specifically, one would expect a user to engage more actively and more intimately under the belief that she is untracked. She may also engage with different types of content than she would if she knew she were being surveilled, exposing them as relevant for further categories of valuable advertising.

103. Tracking users' engagement across Google's advertising products also allows greater optimization of those advertising products, with respect to those individual users, to increase the likelihood of their future engagement with ads, further increasing Google's ability to generate profit.

104. By sending to Google Un-Synced Chrome users' data reflecting their behavior, Google is able to draw a more complete picture of those users, even when they had not opted-in to such tracking.

105. All of this results in concrete, ascertainable financial gain for Google, directly attributable by the increased user engagement. Those profits can be identified and quantified; indeed, teams of analysts at Google are engaged in precisely this process.

E. How Google Instructs Chrome to Report PI to Google

106. Chrome is a web-browser—a software application that enables users to exchange electronic communications over the Internet.

107. Every website is hosted by a computer server through which the entity or person in charge of the website exchanges communications with Internet users via users' web-browsers.

108. The process through which Chrome transmits communications between users and the first-party websites with which users are communications is called packet-switching.[16]

109. The prior technology through which phone communications were transmitted was called circuit-switching. With circuit-switching, the service provider would establish a single pathway (or circuit) through which the content of a communication would flow between the parties to the communication. The problem with circuit-switching is that, if the single path becomes blocked, the communication fails.

110. Enter packet-switching. With packet-switching, there is no single, dedicated path through which the contents of a communication flow. Instead, the contents of a communication are broken down into dozens, hundreds, or thousands of packets—each of which is routed over a network with different paths to the destination. Each packet contains part of the content and information about its destination. Each packet travels independently to the destination and every packet may travel by a different route to the destination. As the packets arrive, they are arranged by the device to which they are sent. Only at the end are they put both together and the communication formed. The path of each packet, and the order in which each packet arrives, is not relevant to the ultimate success of a communication. Some packets may get stopped in the process—in which case they are resent down a different path.

111. Packet-switching is now ubiquitous. For example, all 4G and 5G voice or data communications are made via packet-switching technology.

112. Thus, although common imagination may suppose that a modern cellphone call or internet communication involves a direct line of communication between the participants to the

[16] Packet-switching is also explained in *U.S. v. Szymuszkiewicz,* 622 F.3d 701, 704 (7th Cir. 2010).

communication, that is not true at all. Through packet-switching, the contents of the communication are broken down into dozens, hundreds, or thousands of different packets that are exchanged through separate pathways between the parties to the communication.

113. On the Internet, when a user begins a communication with a website, the user's browser starts and continues several processes all at once. These simultaneous processes include:

a. sending contents of the users' side of the communication to the website;

b. receiving and rendering the website's side of the communication;

c. placing the content of the communication in temporary and intermediate storage, and;

d. in some cases, re-directing the contents of the communication to third-parties;

114. The basic commands that Chrome uses to send the users' side of a communication are called GET and POST requests.

115. When a user types https://www.mercurynews.com/2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/ into her browser (or takes the technological shortcut of clicking a hyperlink), Chrome contacts the website hosting the Mercury News and sends the following communication: "GET 2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/".

116. If instead the user were filling out a form on that website and clicks a button to submit the information in the form, Chrome similarly makes connection with the website server but instead sends a "POST" request that includes the specific content that the user placed in the form.

117. When a user clicks a hyperlink or hits ENTER to send a communication, Chrome determines whether it is a GET or POST request based on the source code within the browser or the current website with which the user is communicating. The browser then simultaneously:

a. Places the contents of the GET or POST request in storage in the browser's web-browsing history and short-term memory; and

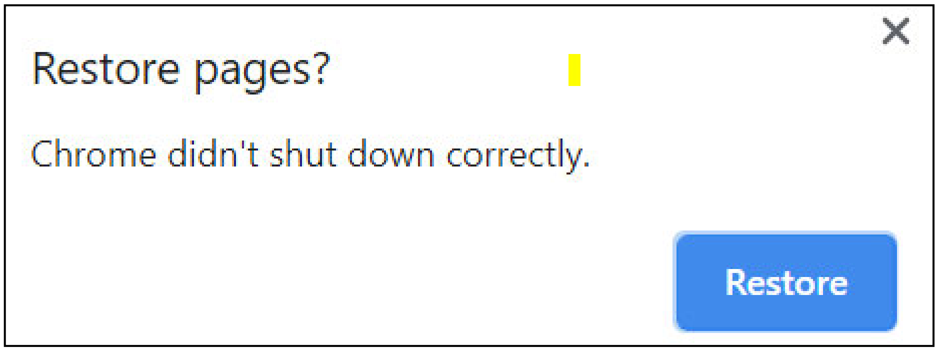
b. Connects to and begins a back-and-forth the two-way communication exchange between the user and the website.

118. Chrome stores the contents of the communication for at least two purposes:

a. content is placed in the browser's short-term memory so that, if the user's web-browser crashes unexpectedly, when the user re-starts their browser, the browser will be able to offer the user the ability to return to their last communications prior to the browser's crash; and

b. The content is placed in the user's browsing history and the user's future reference for 90 days.

119. For short-term memory, if Chrome crashes unexpectedly and the user re-opens it, Chrome provides the user with the following options at the upper right-hand side of the screen:



Restore pages?

Chrome didn't shut down correctly.

120. This short-term storage is for purposes of back-up protection.

121. The storage for 90 days in the user's browsing history is temporary, intermediate storage incidental to the contemporaneous transmission of the communication.

122. In response to receiving a GET or POST request from a user, the server for the website with which the user is exchanging a communication will send a set of instructions to Chrome, commanding Chrome with source code on:

a. How to render the website's portion of the communication; and

b. In some cases (up to 86 percent of popular websites), using source code provided by Google and specifically designed to command the Chrome to contemporaneously re-direct the precise content of the GET or POST part of the communication to Google and its various entities attached to personal information and other browser-generated data about the content of the website's portion of the communication.

123. Google instructs developers to place its source code that commands Chrome to contemporaneously re-direct the contents of the communication exchanged between the user and the website to Google in the website's header—i.e., before the website's instructions regarding the contents of its side of the communication. For example, for Google Tag Manager, Google instructs developers to place its code "as close to the opening <head> tag as possible on every page of your website[.]"[17]

124. Google's placement is designed to put priority on the re-directions of content and user personal information from Chrome to Google. By placing the re-direction commands first, Google ensures that the re-direction will occur as soon as possible so that Google will be able to collect the contents and personal information even if the user quickly changes their mind or the browser unexpectedly shuts down before the communication transmissions are complete.

125. The transmission process between Chrome and the website server is not discrete, but instead involves a series of rapid, continuing, simultaneous data exchanges between Chrome and the website server with data flowing both ways throughout the process and through dozens, hundreds, or even thousands of different paths to reach their destination at the user or website.[18]

126. The data and content exchanges between Chrome and the website server continue even after it appears that the website's portion of the communication has been fully rendered on the user's screen.

127. At the same time that the transmission and content exchange of the communication is happening between the user's browser and the website server (i.e. the devices), the contents of the communication (including the user's specific request and information about the substance of website's side of the communication) are re-directed to third-parties.

[17] *See* https://developers.google.com/tag-manager/quickstart

[18] In one example of which counsel is aware, a recording of a single 288 second communication resulted in 22,779 separate packet transmissions—or 79 data packet transmissions per second.

128. The Google and Chrome browser-generated redirections of the contents of the communication occur:

a. Without any further action of the user;

b. While connections and the contents of the communication are still being exchanged between the user and the website; and

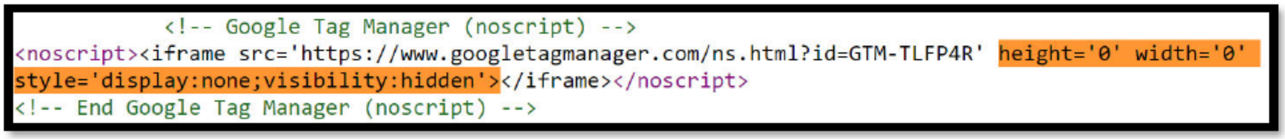
c. Without exception, while the connection between and the communication between the user and the website is still occurring.

129. Google is the most frequent third-party recipient of browser-redirected communications.

130. The Google source code and Chrome browser-generated re-directions of communications content and personal information from Chrome to Google occurs through a combination placement of web-bugs or tracking pixels and iframes.

131. A web-bug or tracking pixel is a 1x1 pixel that is placed on the screen. It is tiny and purposefully designed to remain invisible to the user. The web-bug is a tiny, invisible window through which Google surveils Internet users.

132. An iframe is a container in which a web-developer can place content, or, in the case of Google's source code and surveillance tools, can place source code for web-bugs or tracking pixels. In many cases, Google's source code and Chrome browser-generated re-directions are funneled first through an iframe designed by Google through a service called Google Tag Manager. The source code for Google Tag Manager instructs Chrome to make certain that the surveillance tool is invisible, literally stating that the Google Tag Manager iframe should hidden. For example, here is the Google Tag Manager source code crafted by Google for The Mercury News:



```
           <!-- Google Tag Manager (noscript) -->
<noscript><iframe src='https://www.googletagmanager.com/ns.html?id=GTM-TLFP4R' height='0' width='0'
style='display:none;visibility:hidden'></iframe></noscript>
<!-- End Google Tag Manager (noscript) -->
```

133. Google writes the source code for web-developers to deploy for its invisible web-bugs and tracking pixels, and for Google Tag Manager, a vessel Google developed to make it even easier for websites to deploy its surveillance tools. Then, having designed the source code to

command the contemporaneous re-direction of the contents of communications and user personal information to itself, Google then designed Chrome to send the personal information to Google ***regardless of whether the user is logged-in to Google Sync,*** in violation of Chrome's express promises to users.

134. Chrome sends the following personal information to Google when a user exchanges communications with any website that includes Google surveillance source code—again, ***regardless of whether a user is logged-in to Google Sync or not***:

a. The user's unique, persistent cookie identifiers;

b. The user's browsing history in the form of the contents of the users' GET requests and information relating to the substance, purport, or meaning of the website's portion of the communication with the user;

c. In many cases, the contents of the users' POST communications;

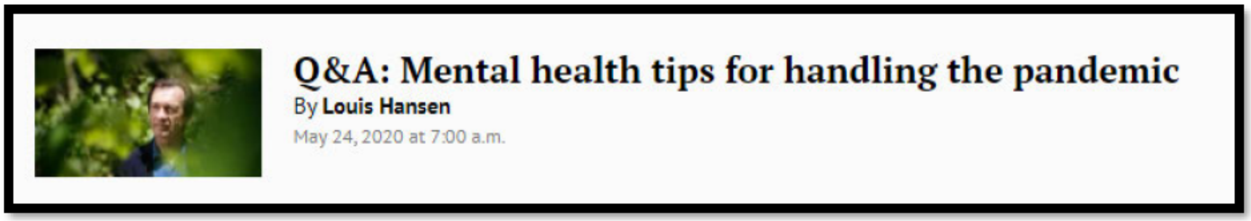
d. The user's IP address and User-Agent information about their device; and

e. The user's x-client-data identifier.

135. Each category of personal information that Chrome sends to Google is a separate violation of Chrome's Terms of Service and an invasion of users' privacy. And the aggregate impact of these takings effectively puts users ***who opted not to Sync*** under Google's surveillance.

F. A Sample Visit to The San Jose Mercury News Website Using Chrome – Comparison Between a "Synched" Session and "Un-synched" Session

136. Suppose a Chrome user wished to access an article on mental health during the Covid-19 pandemic and saw the link below to a relevant article on the San Jose Mercury News, and clicked it:

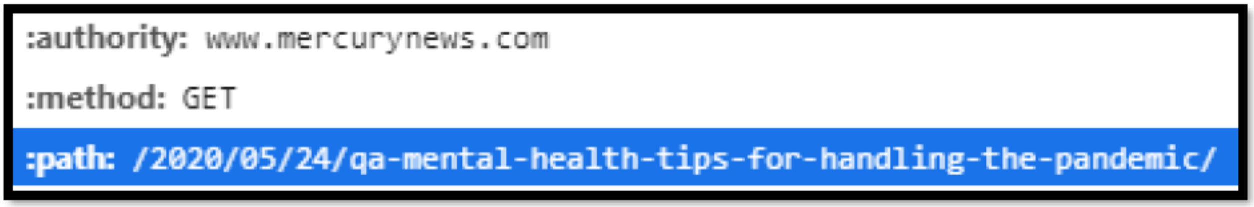


Q&A: Mental health tips for handling the pandemic
By **Louis Hansen**
May 24, 2020 at 7:00 a.m.

137. Immediately upon clicking the link, Chrome places the content of the user's part of the communication in temporary storage, as described above.

138. Chrome also immediately communicates a GET request on behalf of the user to The Mercury News at www.mercurynews.com requesting that The Mercury News exchange its part of the communication by sending a specific article: "Q&A: Mental health tips for handling the pandemic."

139. The specific GET request sent from Chrome to The Mercury News is:



```
:authority: www.mercurynews.com
:method: GET
:path: /2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/
```

140. The user's simple act of clicking a mouse to begin the communication with The Mercury News about Mental Health Tips for Handling the Pandemic triggers a set of contemporaneous, ongoing connections between Chrome and The Mercury News—and the contemporaneous redirection of the contents of the communication between the user and The Mercury News to various Google properties.

141. Google's source code and the Chrome browser then immediately re-direct the content of the user's side of the communication and The Mercury News response to Google Tag Manager, Google Ads, Google DoubleClick, Google Analytics, and Google Captcha.

142. Each re-direction of data from Chrome to Google includes one or more of the following: content of the communication, IP address, user-agent information, x-client-data identifier, and various unique, persistent cookies identified herein.

143. On July 21, 2020, counsel for the Plaintiffs employed an expert to record data transmissions from the Chrome browser to Google in each of three different browser-states for the example GET request to The Mercury News for the mental health article discussed above. The browser-states tested were: (1) Sync mode where the Google test account had logged-in to Google Sync; (2) Basic-browser mode where the Google test account had not logged-in to Google Sync but was logged into a Google account (here, Gmail); and (3) Basic-browser mode where the Google test account was not logged-in to Google Sync and also not logged into any other Google account.

144. The following charts compare the PI that Chrome sends to Google when the browser is one of three states: first, when the user has affirmatively synched with another Google Account (called "synched" below); second, when the user is not synched, but logged into another Google service such as Gmail ("un-synched, with Gmail log-in"); and third, when the user is neither synched nor logged into any other Google account ("un-synched, logged out"). As the test results below confirm, ***Google causes Chrome to send PI to itself even when a Chrome user has not authorized the data collection by synching***.

145. Chrome copies and re-directs the content of the user's GET request (the one asking for the article on mental health) to Google Ads, Google DoubleClick, and Google Analytics in identical fashion ***regardless of whether the user is synched***.

PERSONAL INFORMATION CHROME SENDS TO ALL GOOGLE CONTENT OF COMMUNICATION WITH THE MERCURY NEWS Identical for All Browser-States and All Google Entity Recipients	
Synched	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic
Un-Synched, Gmail Login	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic
Un-Synched, no Gmail Login	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic.html

146. Similarly, the x-client-data header Chrome sends to Google Ads, Google DoubleClick, and Google Analytics is identical ***regardless of whether the user is synched:***

PERSONAL INFORMATION CHROME SENDS TO GOOGLE X-CLIENT-DATA-HEADER Identical for All Browser-States and All Google Entity Recipients Except Analytics	
Synched	CKy1yQEIkbbJAQimtskBCMS2yQEIqZ3KAQjnyMoBCLTLygE=
Un-Synched, Gmail Login	CKy1yQEIkbbJAQimtskBCMS2yQEIqZ3KAQjnyMoBCLTLygE=
Un-Synched, no Gmail Login	CKy1yQEIkbbJAQimtskBCMS2yQEIqZ3KAQjnyMoBCLTLygE=

147. Similarly, the IP address and User-Agent data Chrome sends to Google Ads, Google DoubleClick, and Google Analytics is identical ***regardless of whether the user is synched***.

148. Similarly, the Google Analytics "cid" cookie or "Client ID" that Chrome sends to Google is identical ***regardless of whether the user is synched***:

PERSONAL INFORMATION CHROME SENDS TO ALL GOOGLE "CID" – "CLIENT ID" COOKIE VALUE Identical for All Browser-States and All Google Entity Recipients	
Synched	cid=2007029474.1595353114
Un-Synched, Gmail Login	cid=2007029474.1595353114
Un-Synched, no Gmail Login	cid=2007029474.1595353114

149. The third-party cookie data Chrome sends to Google Ads is identical for at least 11 different persistent, unique cookies for Un-Synched Chrome users regardless of whether signed into Gmail, but not transmitted to Google if the Un-Synched Chrome user is not also logged into Gmail:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE ADS **UNIQUE, PERSISTENT THIRD-PARTY COOKIE VALUES** **Identical for Synched and Un-Synched w/ Gmail Login**	

Synched	SID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEgeQPEJdMF0tShKy
	XCg_BgOS7PQHBWgLiW71F4Q.
	__Secure-3PSID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEge
	QPEJdMF0tShKyXryW3ljJQRAkrQ
	0hbzqbBHg.
	HSID=AFuEZ4mCJy32UrJK7
	SSID=Aw06H6mNsRcQYQjqA
	APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB
	SAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7apJgjE
	__Secure-HSID=AFuEZ4mCJy32UrJK7
	__Secure-SSID=Aw06H6mNsRcQYQjqA
	__Secure-APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB
	__Secure-3PAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7ap
	JgjENID=204=Yc40KkubQ69v_6cmRVkl6eEK6FPzgNcuct
	N7ndjgcsBeMwUO4uxFOCBmFTLG0HNLk7p13a0Le2tnE
	gjOllwZi62Jh4f4fjKFXMR8pL0Z4GqbjlUtejOv3Nvhtf1D
	n63dABgRTnJlRXPklAsY5hCMQfLCHCAKIrg01U
	p3q7q2fFN3Aj8lXaT9g12rT5QtcNgJAZP8dKmLevACA

Un-Synched, Gmail Login	SID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEgeQPEJdMF0tShKy
	XCg_BgOS7PQHBWgLiW71F4Q.
	__Secure-3PSID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEge
	QPEJdMF0tShKyXryW3ljJQRAkrQ
	0hbzqbBHg.
	HSID=AFuEZ4mCJy32UrJK7
	SSID=Aw06H6mNsRcQYQjqA
	APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB
	SAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7apJgjE
	__Secure-HSID=AFuEZ4mCJy32UrJK7
	__Secure-SSID=Aw06H6mNsRcQYQjqA
	__Secure-APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB
	__Secure-3PAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7ap
	JgjENID=204=Yc40KkubQ69v_6cmRVkl6eEK6FPzgNcuct
	N7ndjgcsBeMwUO4uxFOCBmFTLG0HNLk7p13a0Le2tnE
	gjOllwZi62Jh4f4fjKFXMR8pL0Z4GqbjlUtejOv3Nvhtf1D
	n63dABgRTnJlRXPklAsY5hCMQfLCHCAKIrg01U
	p3q7q2fFN3Aj8lXaT9g12rT5QtcNgJAZP8dKmLevACA

Un-Synched, no Gmail Login	none

150. Despite Google’s demonstrated ability above to block the transmission of some cookies, it still causes others to be transmitted, as noted below, ***regardless of whether the user is synched***:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE DOUBLECLICK THIRD-PARTY COOKIES – IDE identical for all browser states	
Synched	IDE=AHWqTUluD72jj7k5Rr5ipWiIeEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV
Un-Synched, Gmail Login	IDE=AHWqTUluD72jj7k5Rr5ipWiIeEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV
Un-Synched, no Gmail Login	IDE=AHWqTUluD72jj7k5Rr5ipWiIeEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV

151. Finally, Chrome sends other third-party cookie personal identifiers that qualify as personal information, ***regardless of whether the user is synched***. These other cookies have values that change based on log-in status, but which are associated with the cookie values that are identical across all browser-states, making them reasonably capable of being associated with specific users:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE DOUBLECLICK COOKIE SYNCHING Identical for All Browser-States	
Synched	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbL6y_qlGA
Un-Synched, Gmail Login	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbL6y_qlGA
Un-Synched, no Gmail Login	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbL6y_qlGA

152. Combined, the data that Google causes Chrome to send to itself (illustrated above) demonstrates that Google has designed Chrome to collect massive amounts of user personal information and linked to websites visited, regardless whether the Chrome user synched.

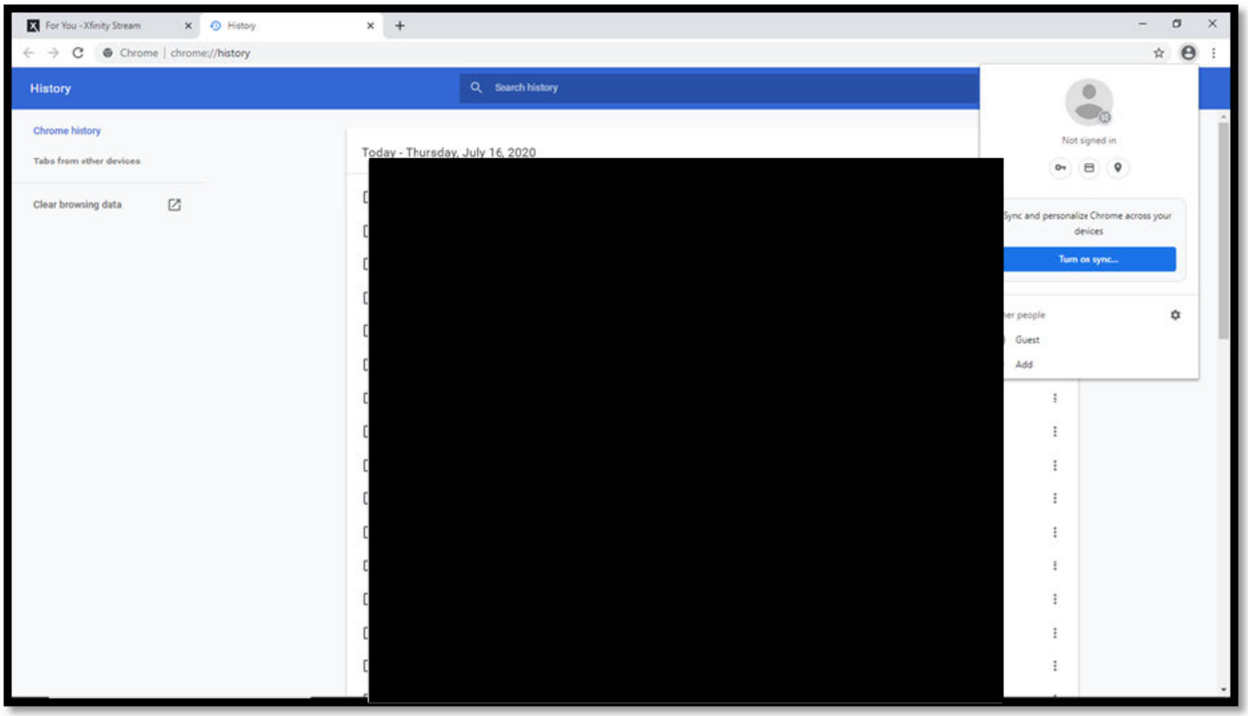
153. Even worse, most of the PI is collected in forms other than cookies (for example, IP address + user-agent data and the x-client-data identifier) meaning that Chrome will still transmit the data even if the user is using cookie blockers.

G. Plaintiffs' Personal Experiences

Plaintiff Patrick Calhoun

154. On Saturday, July 18, 2020, Plaintiff Patrick Calhoun used Fiddler to recreate and record data transmission that Chrome sent from his personal computing device to Google related to websites he had visited earlier in the Relevant Period.

155. Plaintiff Calhoun recorded that, per his usual practice, he was not logged-in to Google Sync at the time of the recording:



For You - Xfinity Stream

History

Chrome | chrome://history

History

Search history

Chrome history

Tabs from other devices

Clear browsing data

Today - Thursday, July 16, 2020

[redacted]

Not signed in

Sync and personalize Chrome across your devices

Turn on sync...

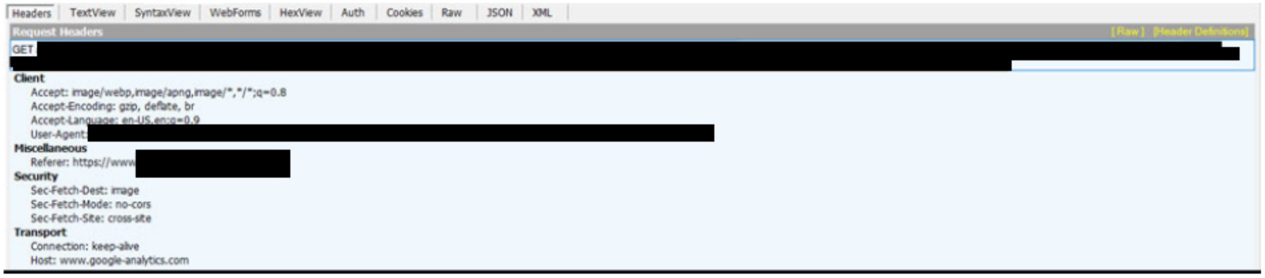
her people

Guest

Add

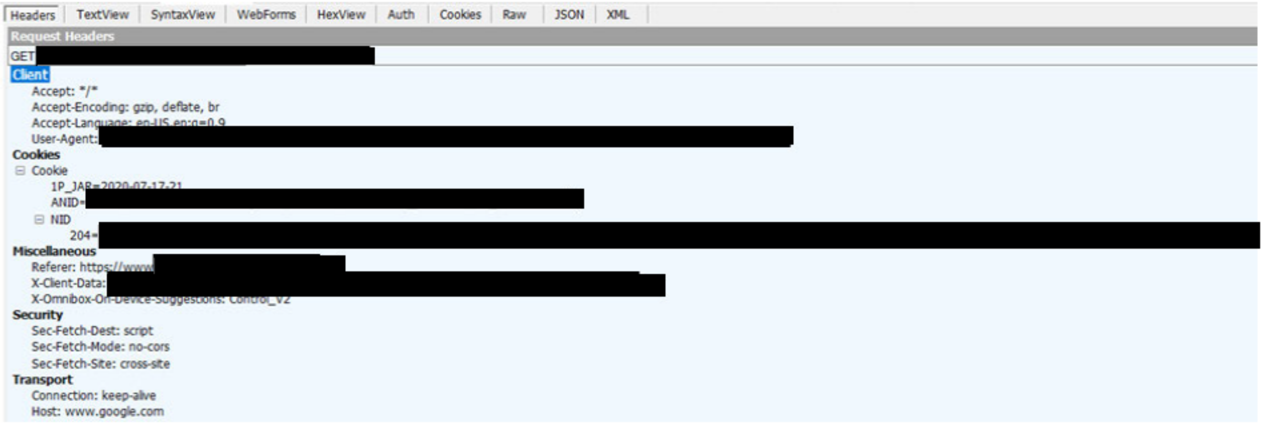
156. Plaintiff Calhoun then recorded data transmissions that Chrome sent to Google when he exchanged communications with [redacted] government and political articles from earlier in the week.

157. For the government communication, Chrome sent the following personal information to Google even though Calhoun was not logged-in to Sync:



```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
Request Headers                                              [Raw] [Header Definitions]
GET [redacted]
Client
    Accept: image/webp,image/apng,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Miscellaneous
    Referer: https://www [redacted]
Security
    Sec-Fetch-Dest: image
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: www.google-analytics.com
```

158. The data Chrome sent to Google Analytics included his IP address, User-Agent information, and CID identifier as well as the content of the communication:



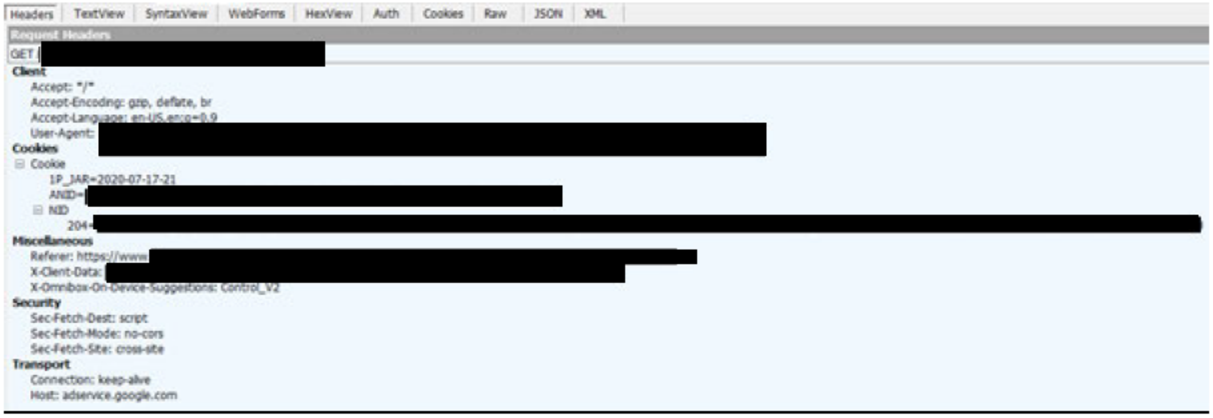
```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
Request Headers
GET [redacted]
Client
    Accept: */*
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        1P_JAR=2020-07-17-21
        ANID= [redacted]
    ⊟ NID
            204= [redacted]
Miscellaneous
    Referer: https://www [redacted]
    X-Client-Data: [redacted]
    X-Omnibox-On-Device-Suggestions: Control_V2
Security
    Sec-Fetch-Dest: script
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: www.google.com
```

159. The data Chrome sent to Google.com included his IP address, User-Agent information, X-Client-Data identifier, uniqe cookie identifiers as well as the content of the communication—a request to load the webpage for the [redacted] all of which Google is aware through its web-crawlers:

[redacted]

160. In addition to Calhoun's personal information about his [redacted] communication with the [redacted], Chrome also sent to Google the exact date and time of Calhoun's communication. Over time, Chrome would disclose the exact date and time of every time Calhoun went to this website.

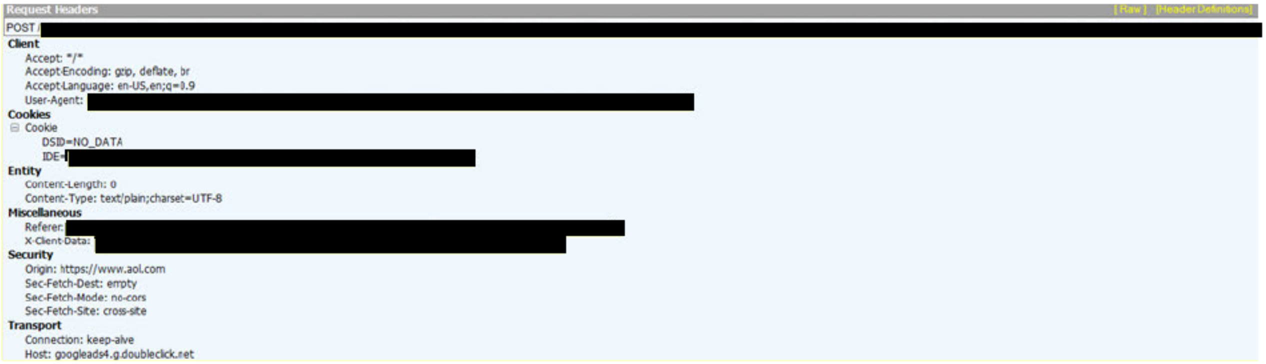
161. For the article of political interest, Chrome sent the following information to Google.com even though Calhoun was not logged-in to Sync:



```
Request Headers
GET [redacted]
Client
    Accept: */*
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        1P_JAR=2020-07-17-21
        ANID=[redacted]
    ⊟ NID
          204-[redacted]
Miscellaneous
    Referer: https://www[redacted]
    X-Client-Data: [redacted]
    X-Omnibox-On-Device-Suggestions: Control_V2
Security
    Sec-Fetch-Dest: script
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: adservice.google.com
```

162. The X-Client-Data identifier, IP address, User-Agent, and NID cookie sent to Google for this communication is identical to the PI Chrome sent to Google following Calhoun's visit to the prior website (allowing his web browsing history to be comprehensively monitored), except here, the content of the communication in the URL is different.

163. Chrome also improperly sent the following PI to Google DoubleClick:



```
Request Headers
POST /[redacted]
Client
    Accept: */*
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
      DSID=NO_DATA
      IDE=[redacted]
Entity
    Content-Length: 0
    Content-Type: text/plain;charset=UTF-8
Miscellaneous
    Referer: [redacted]
    X-Client-Data: [redacted]
Security
    Origin: https://www.aol.com
    Sec-Fetch-Dest: empty
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: googleads4.g.doubleclick.net
```

164. Once again, the X-Client-Data identifier, IP address, and User-Agent sent to Google DoubleClick for this communication is identical to the personal information Chrome sent to Google at the prior website, allowing for association of multiple websites with the same person.

165. In addition, the IDE cookie identifier is identical to the IDE cookie identifier that Chrome would share with Google DoubleClick for communication with a communication exchanged with a website that has deployed Google's DoubleClick source code.

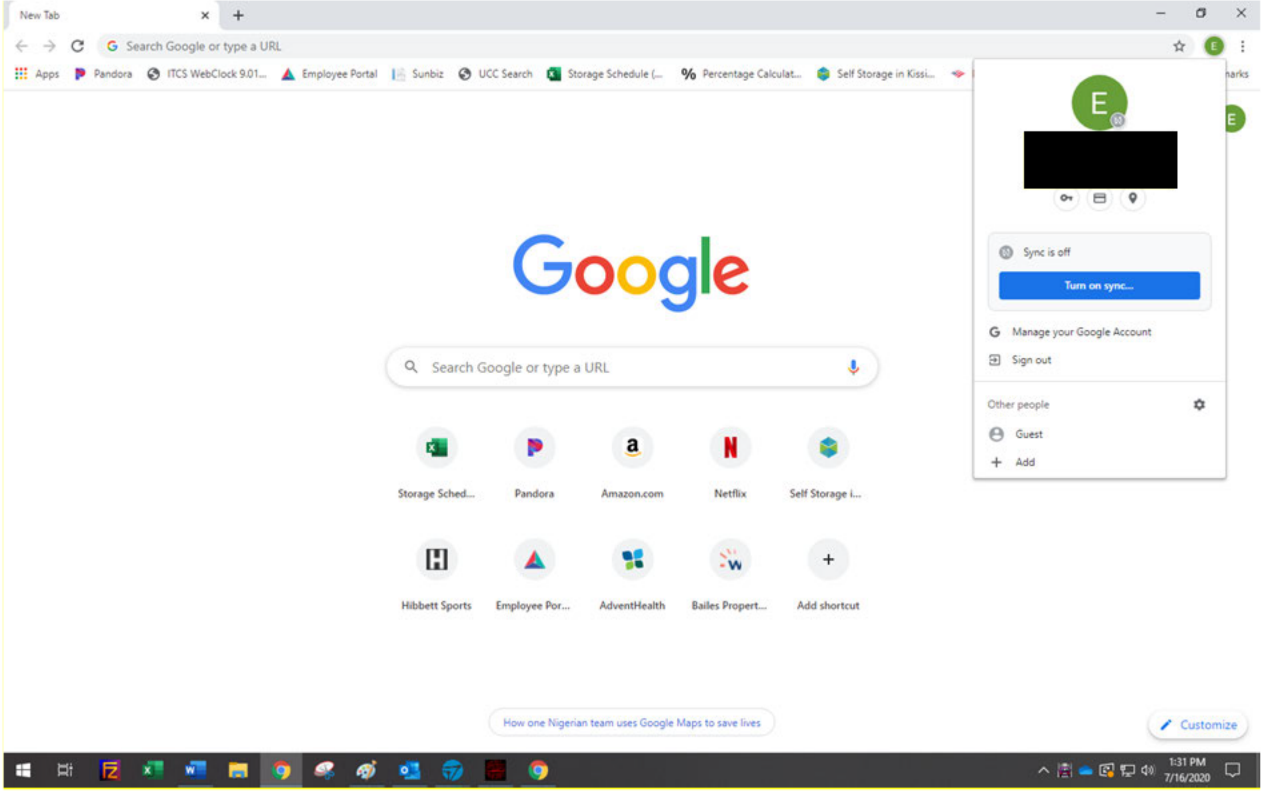
166. Further, Chrome disclosed an "adsid" cookie synching value that would be identical if Calhoun had actually been logged-in to Google Sync.

167. Despite its promises to the contrary, Google combined Plaintiff Calhoun's personal information that it obtained when he was not logged-in to Google Sync with other data it has about him, and will use that data to place Calhoun in advertising categories from which Google will profit from targeted advertising to him based on data that it did not have the right to obtain—including but not limited to recordings captured and detailed herein, that Calhoun communicates with the [redacted] and that he reads political articles with [redacted]

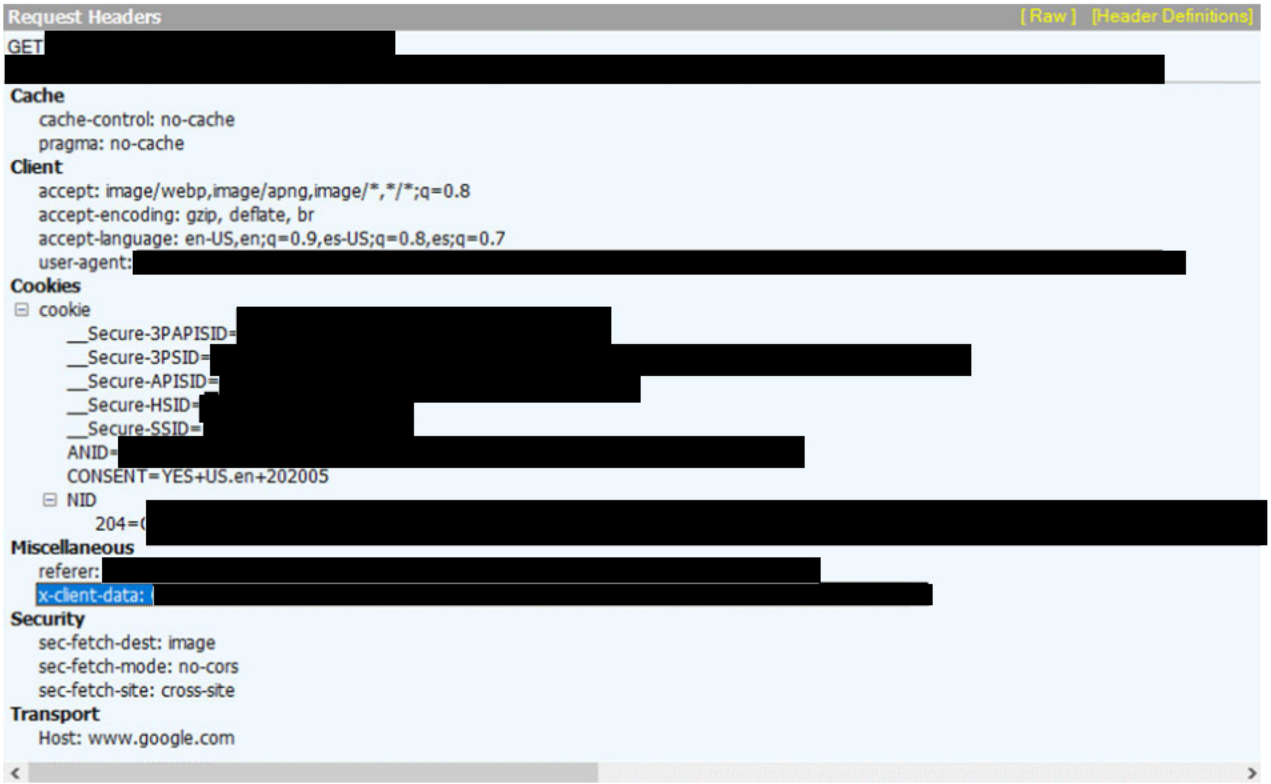
Plaintiff Elaine Crespo

168. On Friday, July 17, 2020, Plaintiff Elaine Crespo used Fiddler to recreate and record data transmissions that Chrome sent from her personal computing device to Google related to websites she had visited earlier in the Relevant Period.

169. Plaintiff Crespo recorded that, per her usual practice, she was not logged-in to Google Sync at the time of the recording:

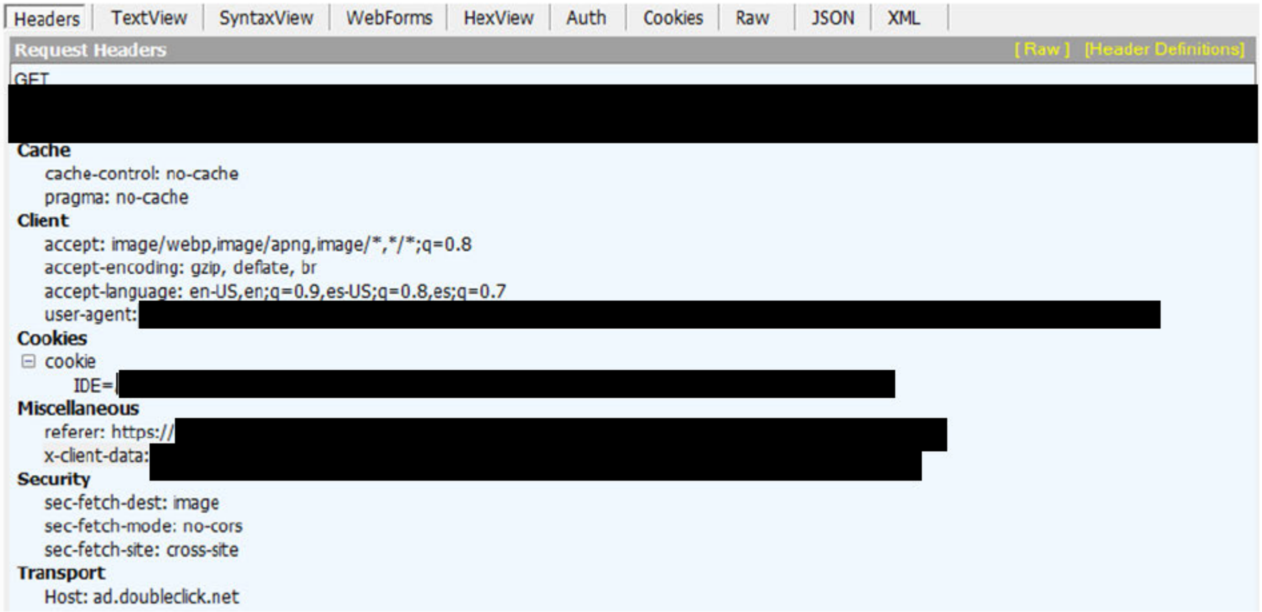


170. Plaintiff Crespo then recorded data transmissions that Chrome sent to Google when she exchanged Internet communications with her bank. She recorded that Chrome sent the following personal information to Google even though Crespo was not logged-in to Sync:



```
Request Headers                                    [ Raw ]  [Header Definitions]
GET [redacted]
Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
    user-agent: [redacted]
Cookies
 ⊟ cookie
        __Secure-3PAPISID=[redacted]
        __Secure-3PSID=[redacted]
        __Secure-APISID=[redacted]
        __Secure-HSID=[redacted]
        __Secure-SSID=[redacted]
        ANID=[redacted]
        CONSENT=YES+US.en+202005
    ⊟ NID
            204=([redacted]
Miscellaneous
    referer: [redacted]
    x-client-data: ([redacted]
Security
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
Transport
    Host: www.google.com
```

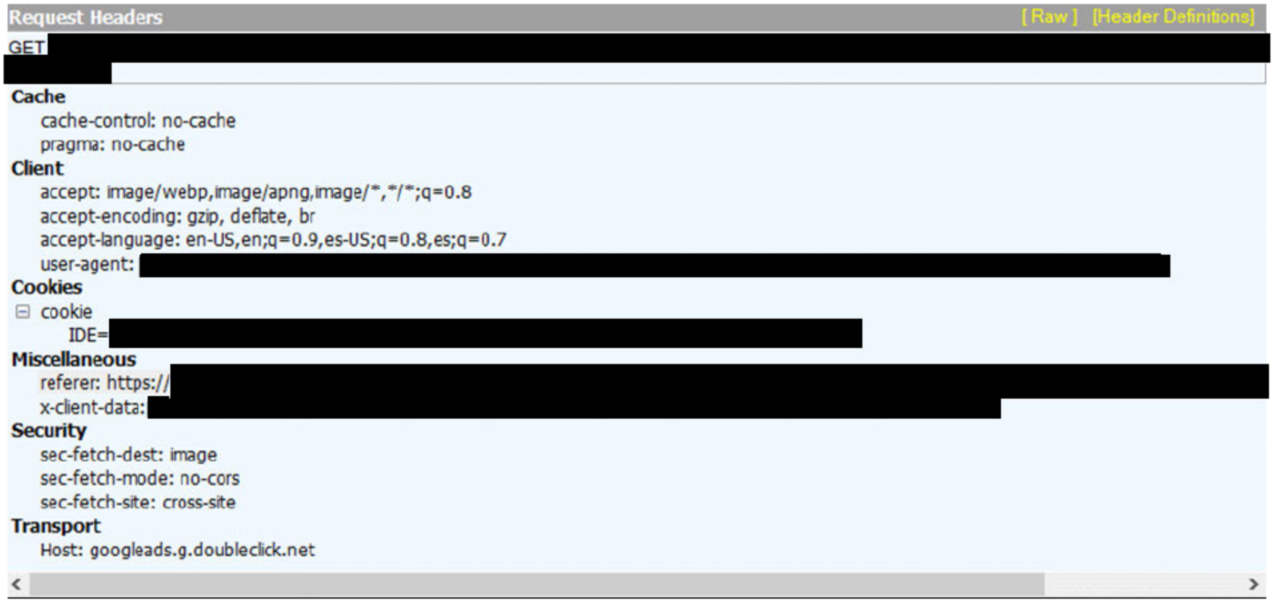
171. Google also caused Chrome to send the following to Google:



Request Headers

GET [redacted]

Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
    user-agent: [redacted]
Cookies
    ⊟ cookie
        IDE=[redacted]
Miscellaneous
    referer: https://[redacted]
    x-client-data: [redacted]
Security
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
Transport
    Host: ad.doubleclick.net

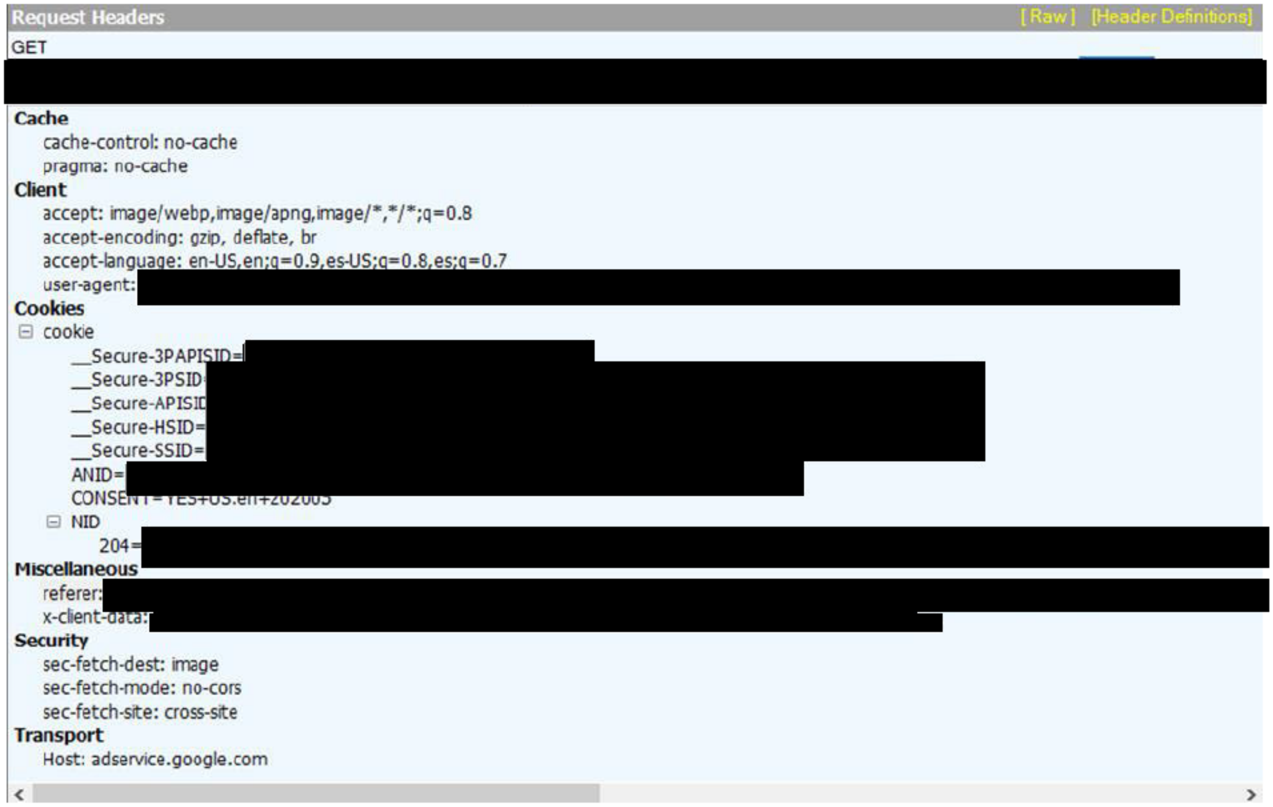


Request Headers

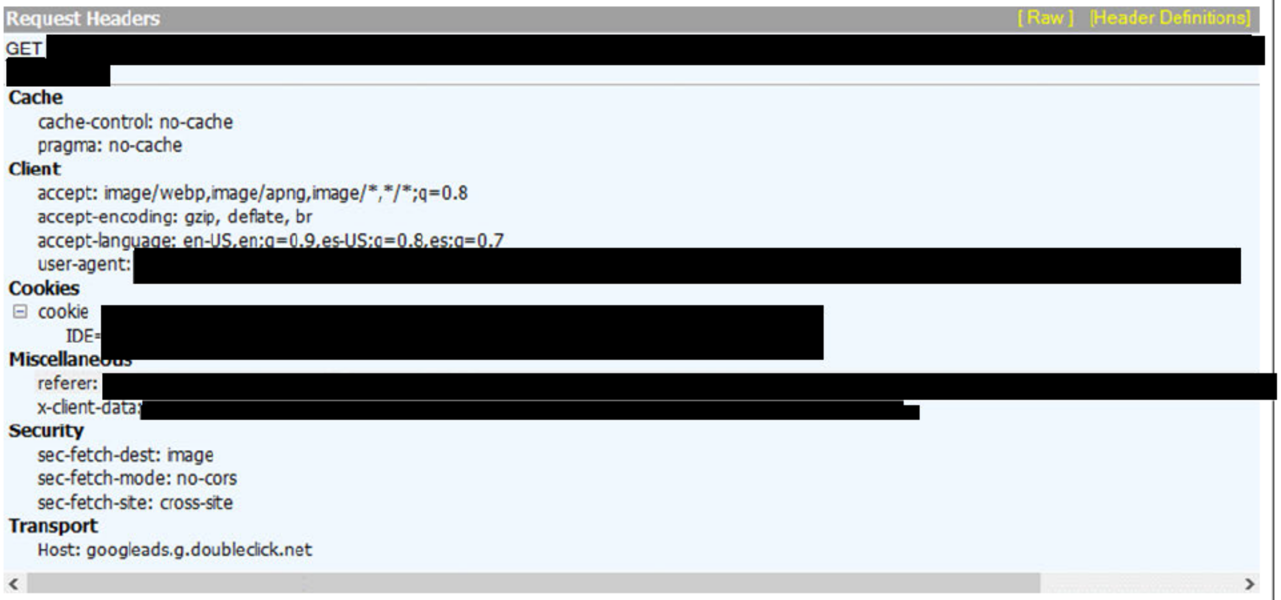
GET [redacted]

Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
    user-agent: [redacted]
Cookies
    ⊟ cookie
        IDE=[redacted]
Miscellaneous
    referer: https://[redacted]
    x-client-data: [redacted]
Security
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
Transport
    Host: googleads.g.doubleclick.net

172. When Crespo logged-out of her bank account, Google knew, at the exact moment it happened, because Chrome improperly shared this fact and other PI with Google Ads and Google DoubleClick.



```
GET
[redacted]
Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
    user-agent: [redacted]
Cookies
⊟  cookie
        __Secure-3PAPISID=[redacted]
        __Secure-3PSID[redacted]
        __Secure-APISID
        __Secure-HSID=
        __Secure-SSID=
        ANID=[redacted]
        CONSENT=YES+US.en+202005
    ⊟  NID
            204=[redacted]
Miscellaneous
    referer:[redacted]
    x-client-data:[redacted]
Security
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
Transport
    Host: adservice.google.com
```



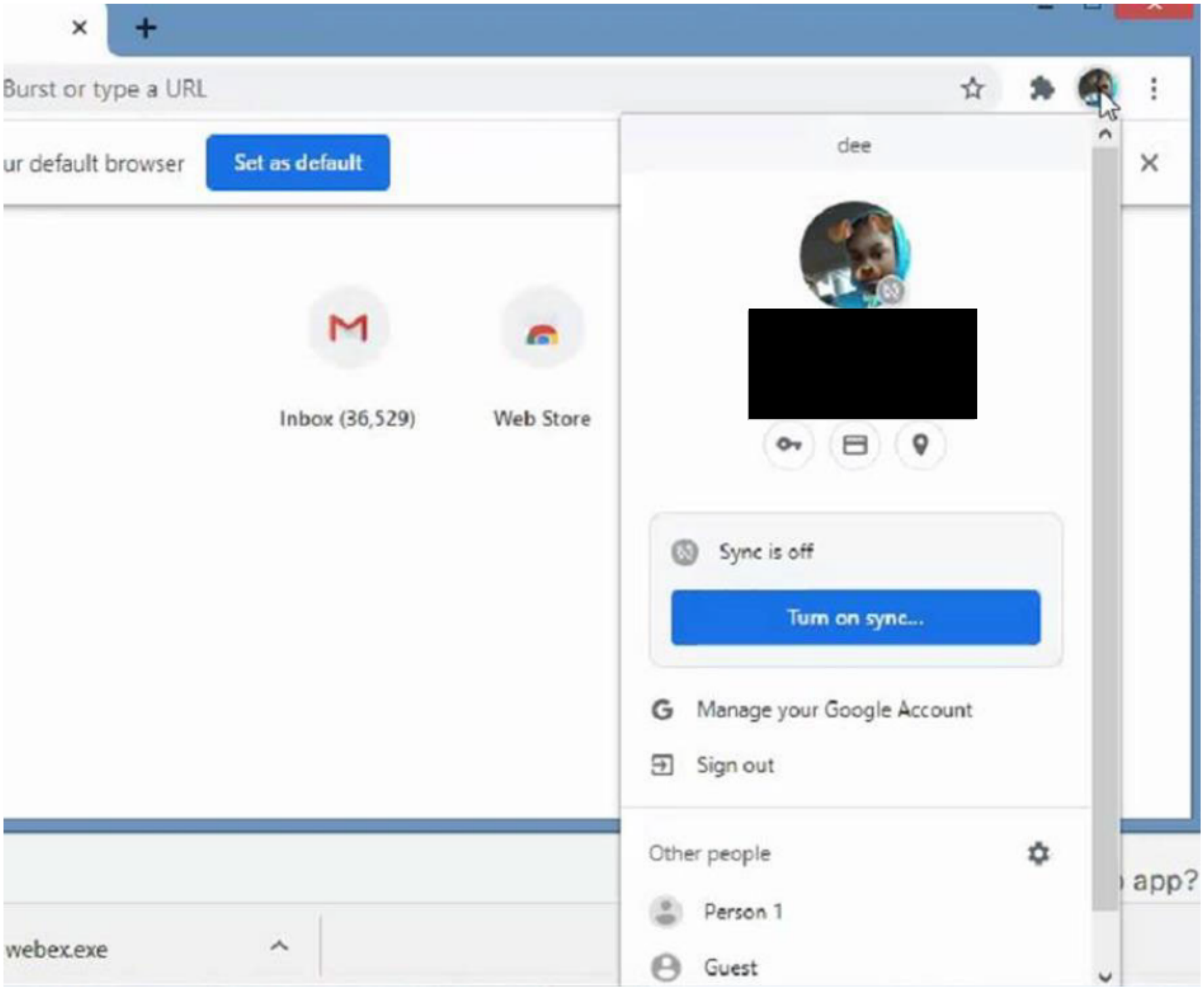
```
GET [redacted]
Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
    user-agent: [redacted]
Cookies
⊟  cookie
        IDE=[redacted]
Miscellaneous
    referer: [redacted]
    x-client-data:[redacted]
Security
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
Transport
    Host: googleads.g.doubleclick.net
```

173. Despite its promises to the contrary, Google combined Plaintiff Crespo's PI that it obtained when she was not logged-in to Google Sync with other data it has about her, and will use that data to place her in advertising categories from which Google will profit from targeted advertising to her based on data that it did not have the right to obtain.

Plaintiff Hadiyah Jackson

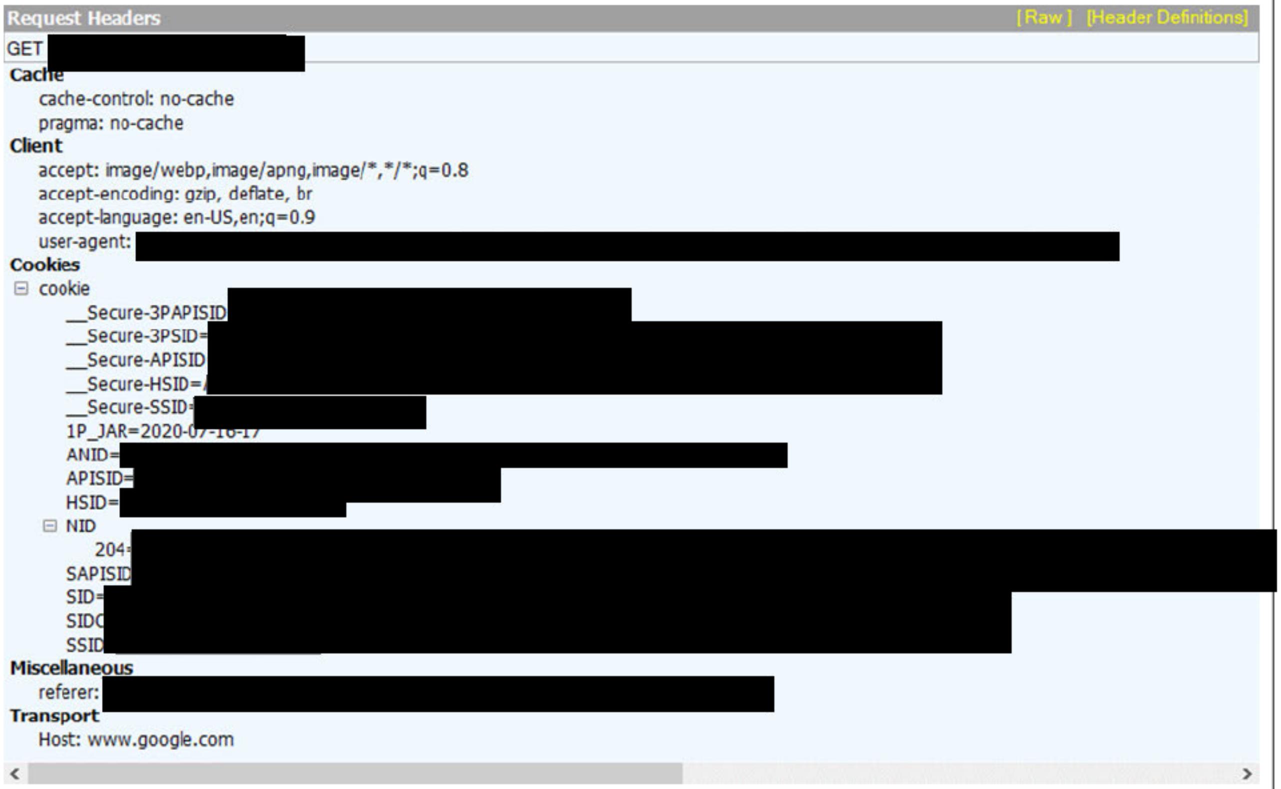
174. On Thursday, July 16, 2020, Plaintiff Hadiyah Jackson used Fiddler to recreate and record data transmissions that Chrome sent from her personal computing device to Google related to websites she had visited earlier in the Relevant Period.

175. Plaintiff Jackson recorded that, per her usual practice, she was not logged-in to Google Sync at the time of the recording:



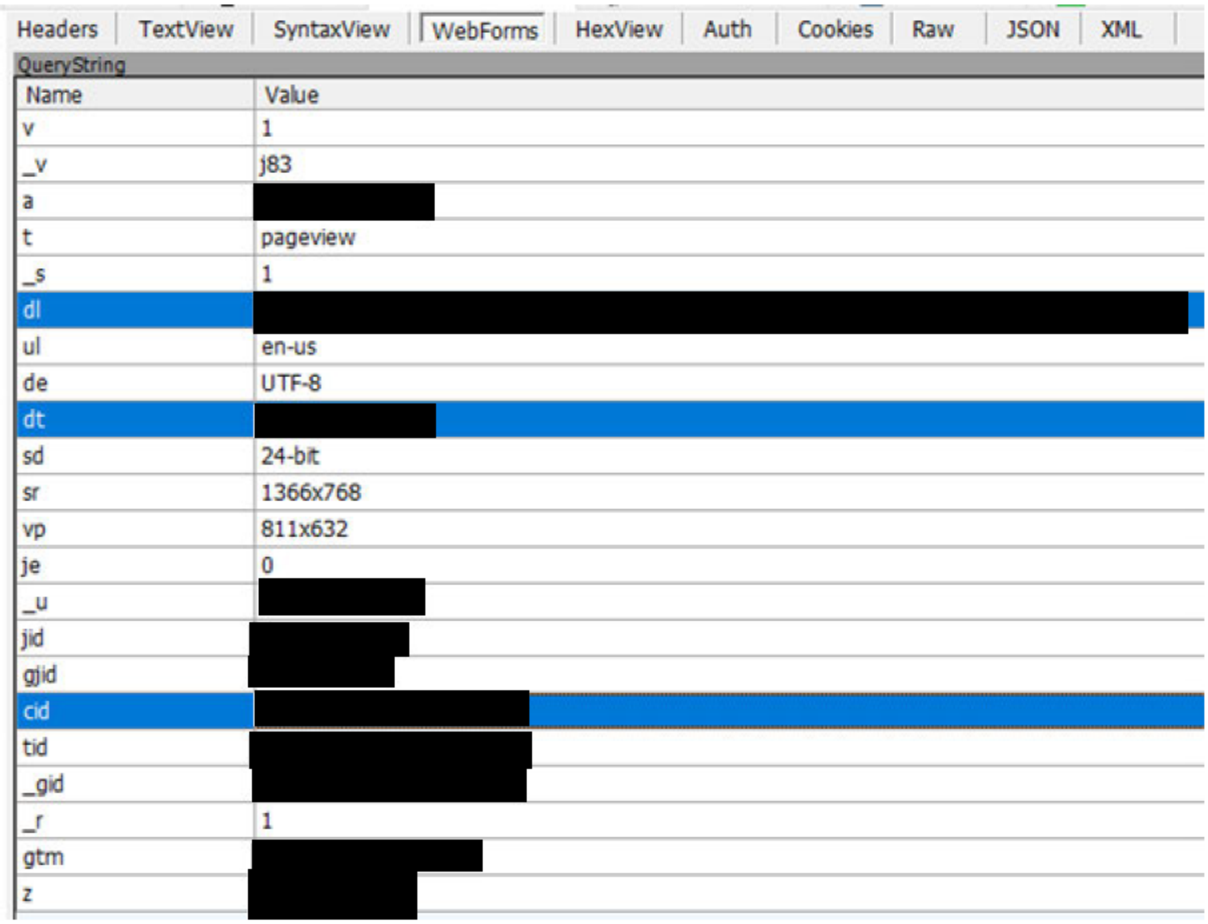
176. Plaintiff Jackson then recorded data transmissions that Chrome sent to Google with the exchange of communications with [redacted] government.

177. For the government communications, Chrome sent the following personal information to Google even though Jackson was not logged-in to Sync:



```
Request Headers                                    [ Raw ]  [Header Definitions]
GET [redacted]
Cache
    cache-control: no-cache
    pragma: no-cache
Client
    accept: image/webp,image/apng,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9
    user-agent: [redacted]
Cookies
⊟ cookie
        __Secure-3PAPISID[redacted]
        __Secure-3PSID=[redacted]
        __Secure-APISID
        __Secure-HSID=
        __Secure-SSID[redacted]
        1P_JAR=2020-07-16-17
        ANID=[redacted]
        APISID=[redacted]
        HSID=[redacted]
    ⊟ NID
            204[redacted]
        SAPISID
        SID=
        SIDC
        SSID
Miscellaneous
    referer: [redacted]
Transport
    Host: www.google.com
```

178. Chrome also improperly sent the following PI to Google Analytics:



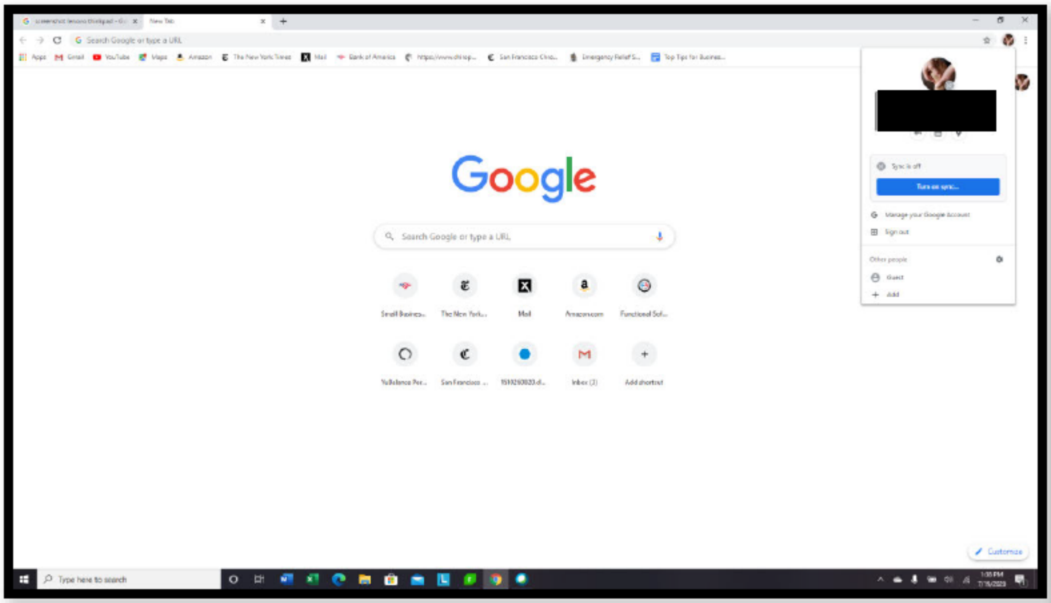
Name	Value
v	1
_v	j83
a	[redacted]
t	pageview
_s	1
dl	[redacted]
ul	en-us
de	UTF-8
dt	[redacted]
sd	24-bit
sr	1366x768
vp	811x632
je	0
_u	[redacted]
jid	[redacted]
gjid	[redacted]
cid	[redacted]
tid	[redacted]
_gid	[redacted]
_r	1
gtm	[redacted]
z	[redacted]

179. Despite its promises to the contrary, Google combined Plaintiff Jackson's personal information that it obtained when she was not logged-in to Google Sync, including communications relating to [redacted] with other data it has about her, and will use that data to place Jackson in advertising categories from which Google will profit from targeted advertising to her based on data that it did not have the right to obtain.

Plaintiff Claudia Kindler

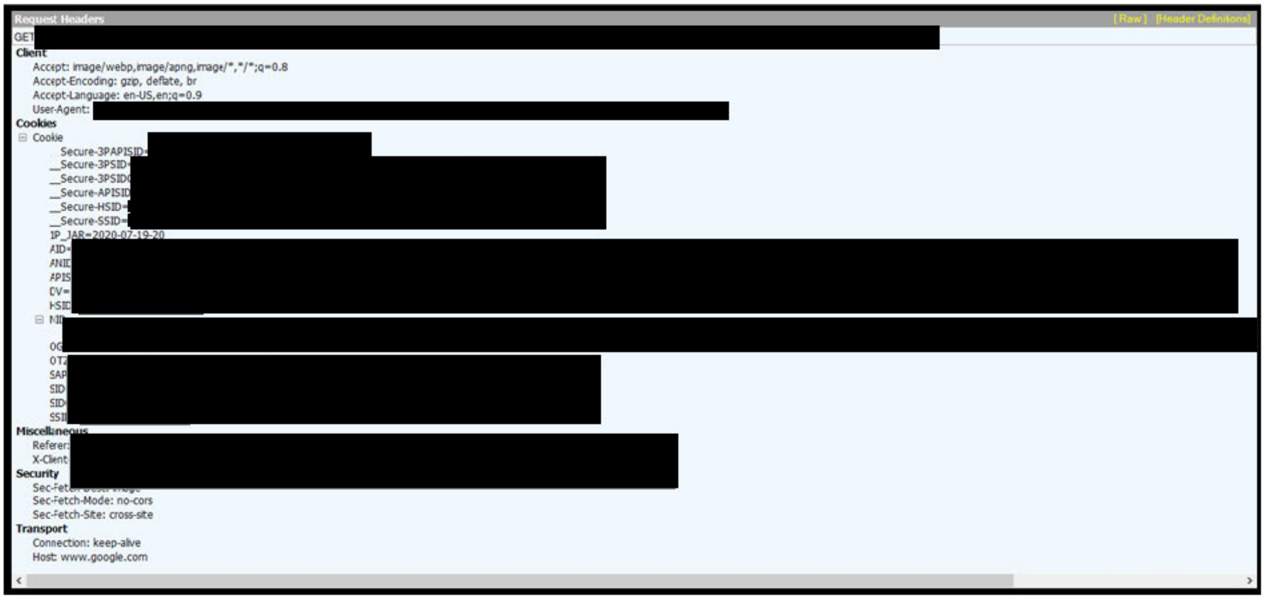
180. On Sunday, July 19, 2020, Plaintiff Claudia Kindler used special software called Fiddler to recreate and record data transmissions that Chrome sent from her personal computing device to Google while visiting websites that she had visited earlier in the Relevant Period.

181. Plaintiff Kindler recorded that, per her usual practice, she was not logged-in to Google Sync at the time of the recording:



182. Plaintiff Kindler then recorded data transmissions that Chrome sent to Google when she exchanged communications with her healthcare provider, her bank, and her continuing professional education provider.

183. For her healthcare provider, Chrome sent the following PI to Google despite the fact that Kindler was not logged-in to Sync:



```
Request Headers                                              [ Raw ]  [Header Definitions]
GET [redacted]
Client
    Accept: image/webp,image/apng,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        Secure-3PAPISID=[redacted]
      __Secure-3PSID
      __Secure-3PSIDC
      __Secure-APISID
      __Secure-HSID=
      __Secure-SSID=[redacted]
      1P_JAR=2020-07-19-20
      AID=
      ANID
      APIS
      DV=
      HSID[redacted]
   ⊟ NI[redacted]
      OG
      OT
      SAP
      SID
      SID
      SSI[redacted]
Miscellaneous
    Referer:
    X-Client
Security
    Sec-Fet[redacted]
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: www.google.com
```

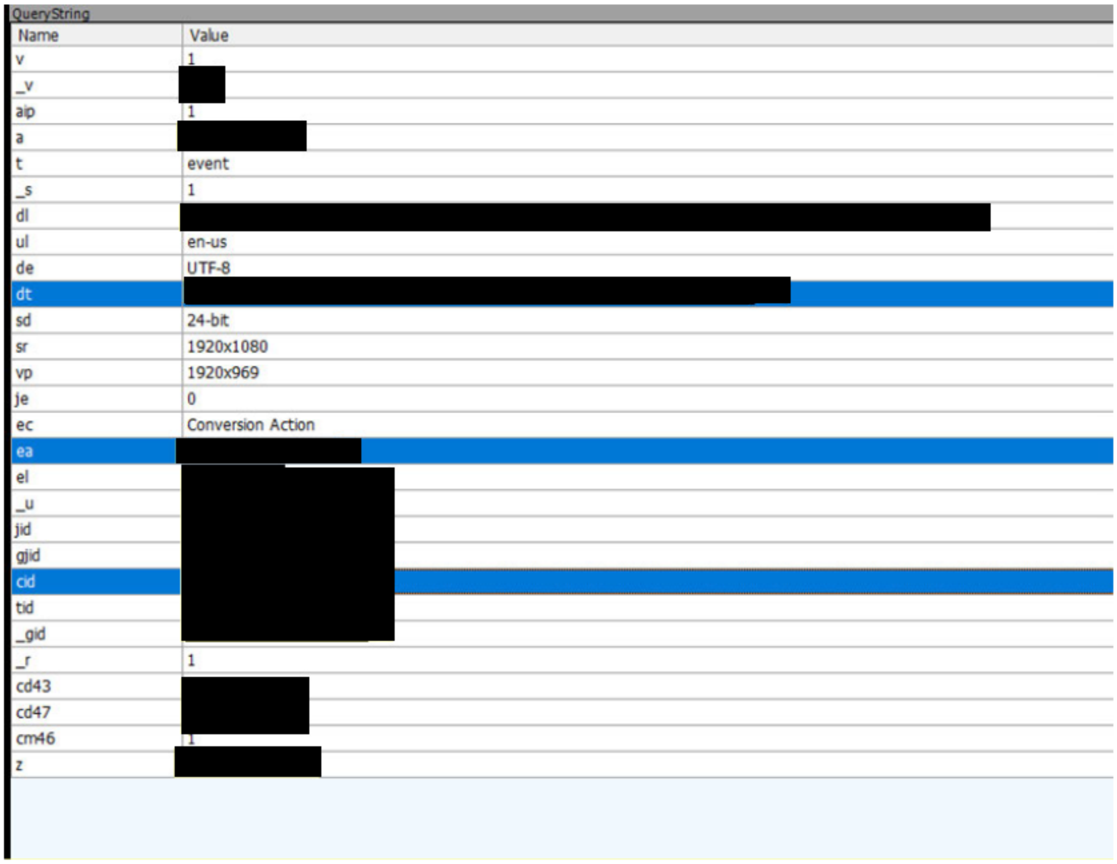
184. Although she was not logged-in to Sync, Chrome disclosed Kindler's personal information to Google that included the fact that Kindler was communicating with her healthcare

provider, the X-Client-Data-identifier, IP address, User-Agent, the cookie-synching “cid” value, and 11 different Google.com cookies that are also associated with her Google account.

185. At the time of the communication, the website would have appeared like this—with the option to reserve a spot at an [redacted]

[redacted]

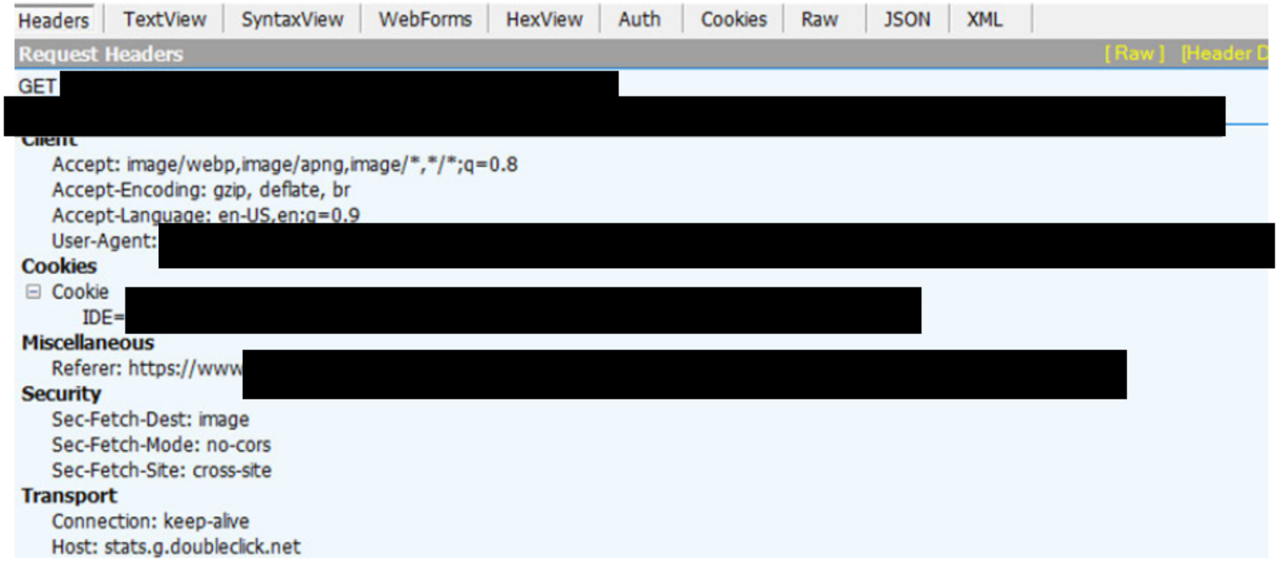
186. When Kindler took action to “Save [Her] Spot at [redacted]” Chrome sent the following PI to Google Analytics:



QueryString

Name	Value
v	1
_v	[redacted]
aip	1
a	[redacted]
t	event
_s	1
dl	[redacted]
ul	en-us
de	UTF-8
dt	[redacted]
sd	24-bit
sr	1920x1080
vp	1920x969
je	0
ec	Conversion Action
ea	[redacted]
el	[redacted]
_u	[redacted]
jid	[redacted]
gjid	[redacted]
cid	[redacted]
tid	[redacted]
_gid	[redacted]
_r	1
cd43	[redacted]
cd47	[redacted]
cm46	1
z	[redacted]

187. Chrome also contemporaneously sent the following PI to Google DoubleClick:



Request Headers

GET [redacted]

[redacted]

Client

Accept: image/webp,image/apng,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
User-Agent: [redacted]

Cookies

⊟ Cookie
IDE=[redacted]

Miscellaneous

Referer: https://www[redacted]

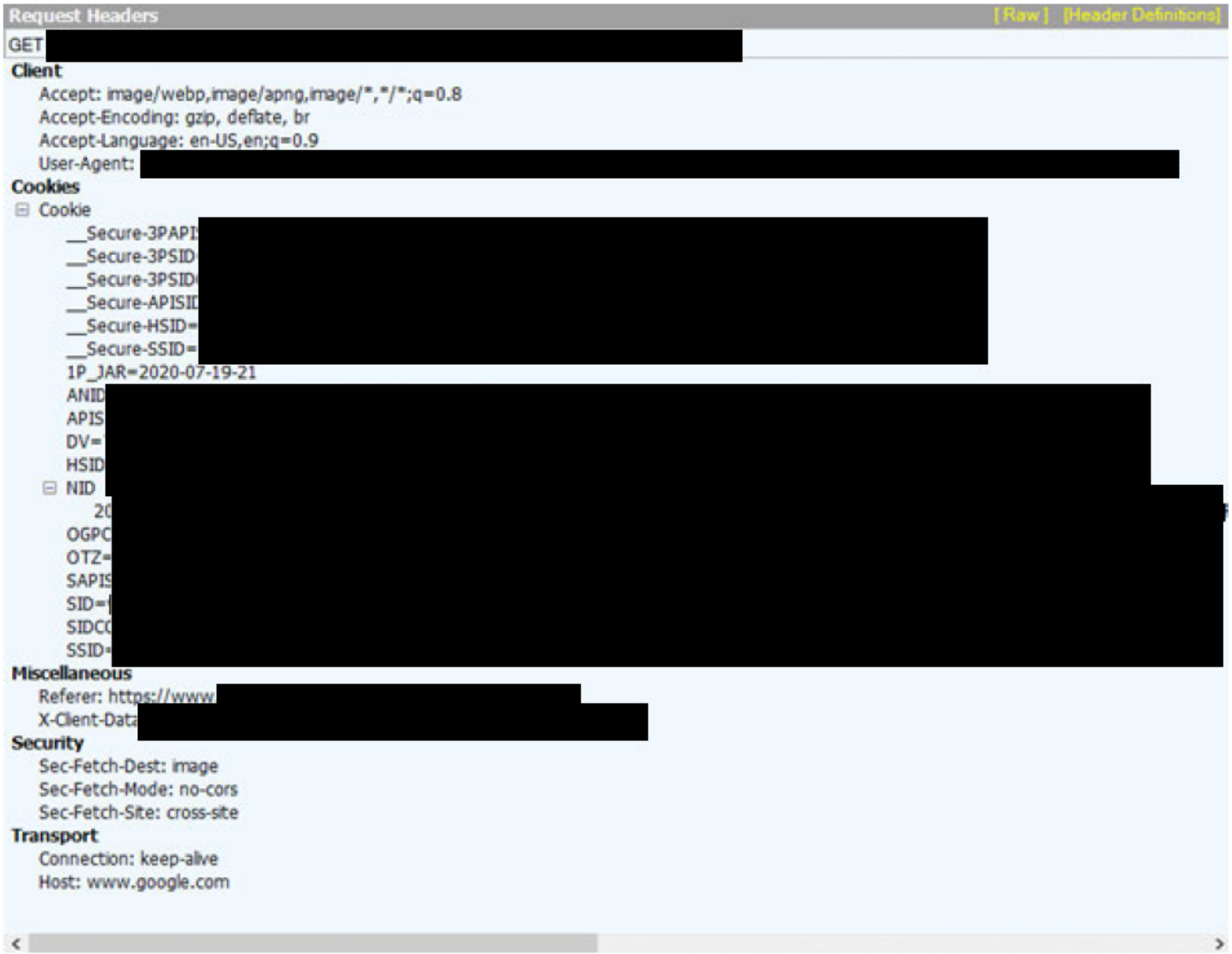
Security

Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site

Transport

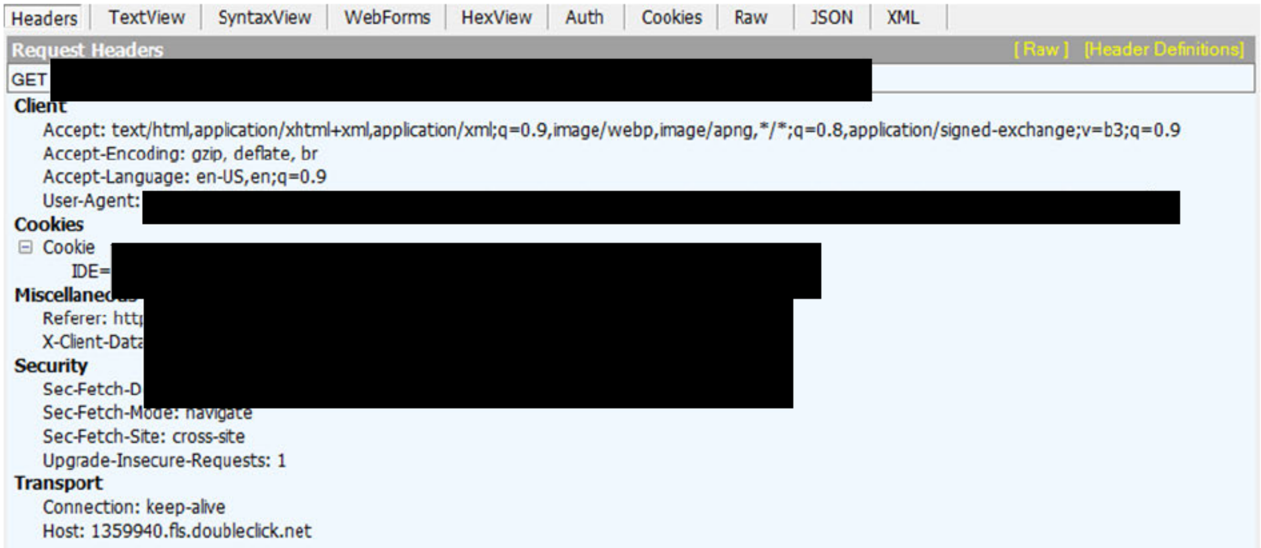
Connection: keep-alive
Host: stats.g.doubleclick.net

188. When she visited her bank's website, Chrome improperly sent the following personal information to Google even though Kindler was not logged-in to Sync:



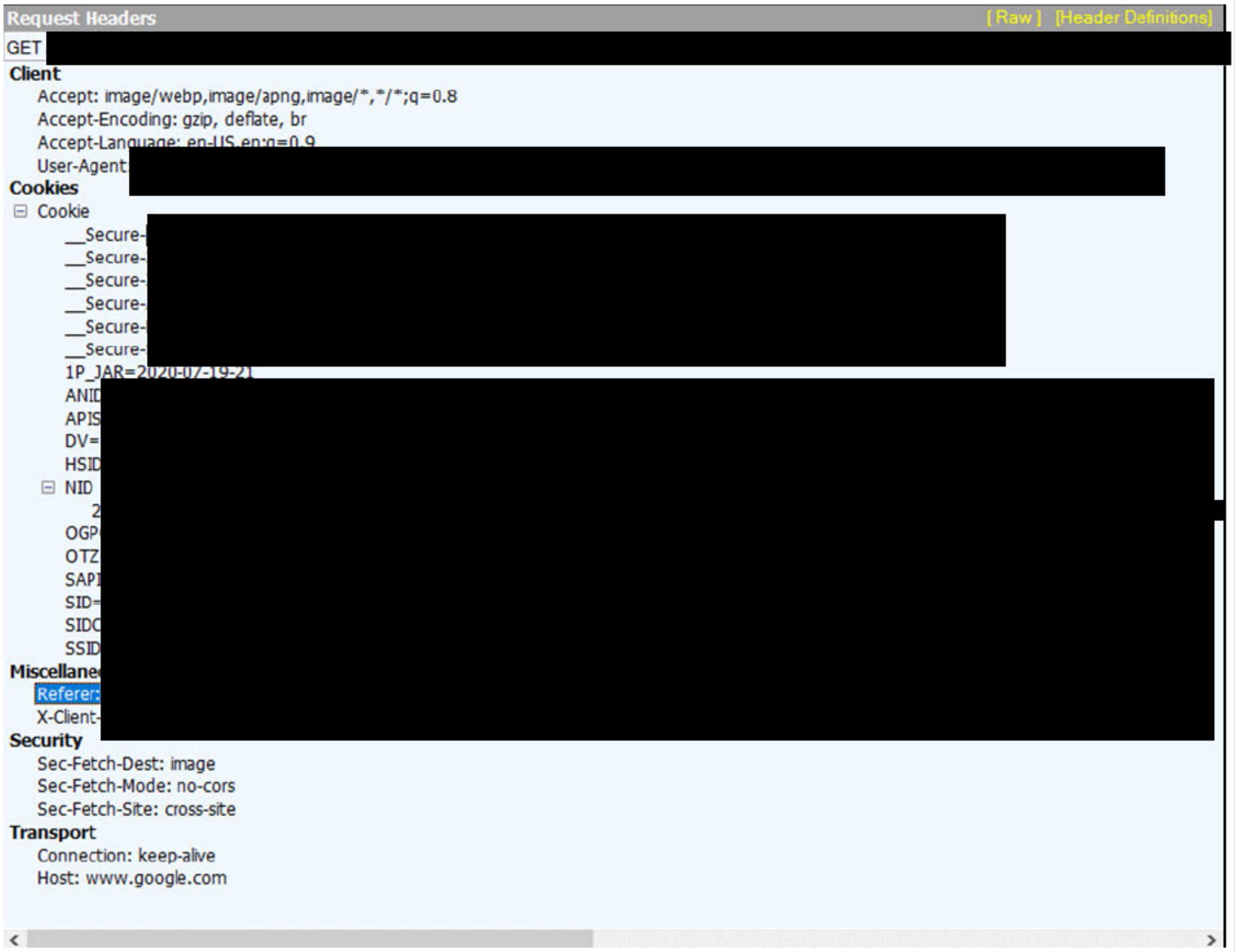
```
Request Headers                                              [ Raw ]  [Header Definitions]
GET [redacted]
Client
    Accept: image/webp,image/apng,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        __Secure-3PAPI
        __Secure-3PSID
        __Secure-3PSID
        __Secure-APISI
        __Secure-HSID=
        __Secure-SSID= [redacted]
        1P_JAR=2020-07-19-21
        ANID
        APIS
        DV=
        HSID
    ⊟ NID
            2
        OGPC
        OTZ=
        SAPIS
        SID=
        SIDCC
        SSID= [redacted]
Miscellaneous
    Referer: https://www
    X-Client-Data [redacted]
Security
    Sec-Fetch-Dest: image
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: www.google.com
```

189. When Kindler logged-out of her banking account, Chrome even informed Google of this fact:



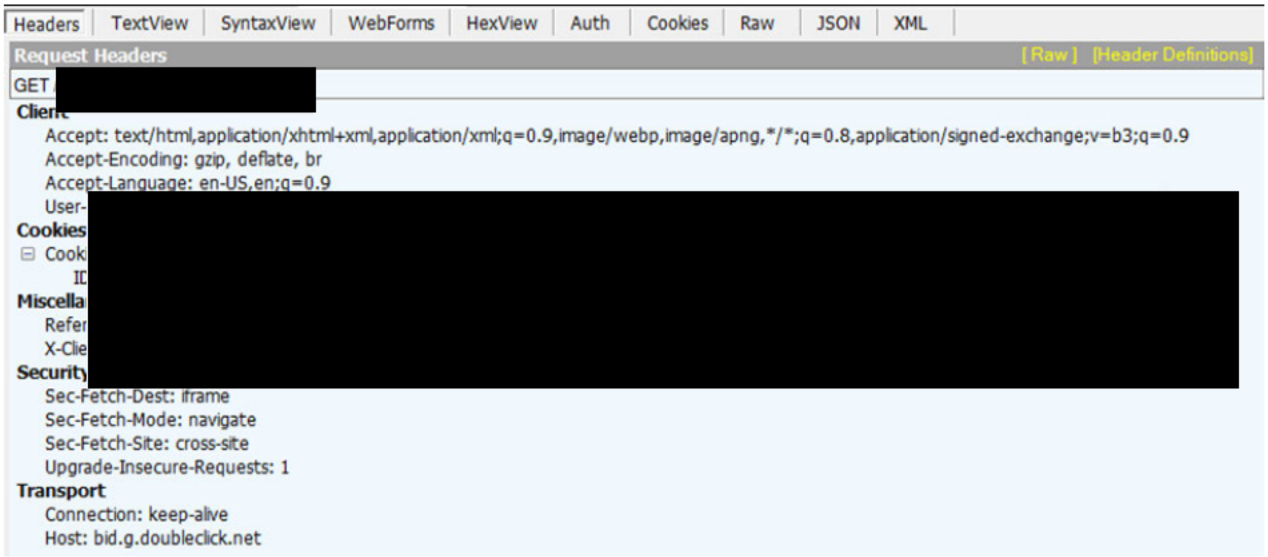
```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
Request Headers                                              [ Raw ]  [Header Definitions]
GET [redacted]
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        IDE= [redacted]
Miscellaneo
    Referer: htt
    X-Client-Data
Security
    Sec-Fetch-D
    Sec-Fetch-Mode: navigate
    Sec-Fetch-Site: cross-site
    Upgrade-Insecure-Requests: 1
Transport
    Connection: keep-alive
    Host: 1359940.fls.doubleclick.net
```

190. When she visited the website of her continuing education provider, once again Google was her uninvited guest, monitoring every step and improperly collecting the following PI despite the fact that Kindler was not Synched with any Google account:



```
GET [redacted]
Client
    Accept: image/webp,image/apng,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-Agent: [redacted]
Cookies
⊟ Cookie
        __Secure- [redacted]
        __Secure-
        __Secure-
        __Secure-
        __Secure-
        __Secure-
        1P_JAR=2020-07-19-21
        ANID [redacted]
        APIS
        DV=
        HSID
    ⊟ NID
            2
        OGP
        OTZ
        SAPI
        SID=
        SIDC
        SSID
Miscellane
    Referer:
    X-Client-
Security
    Sec-Fetch-Dest: image
    Sec-Fetch-Mode: no-cors
    Sec-Fetch-Site: cross-site
Transport
    Connection: keep-alive
    Host: www.google.com
```

191. Chrome also sent Kindler's personal information to Google DoubleClick:

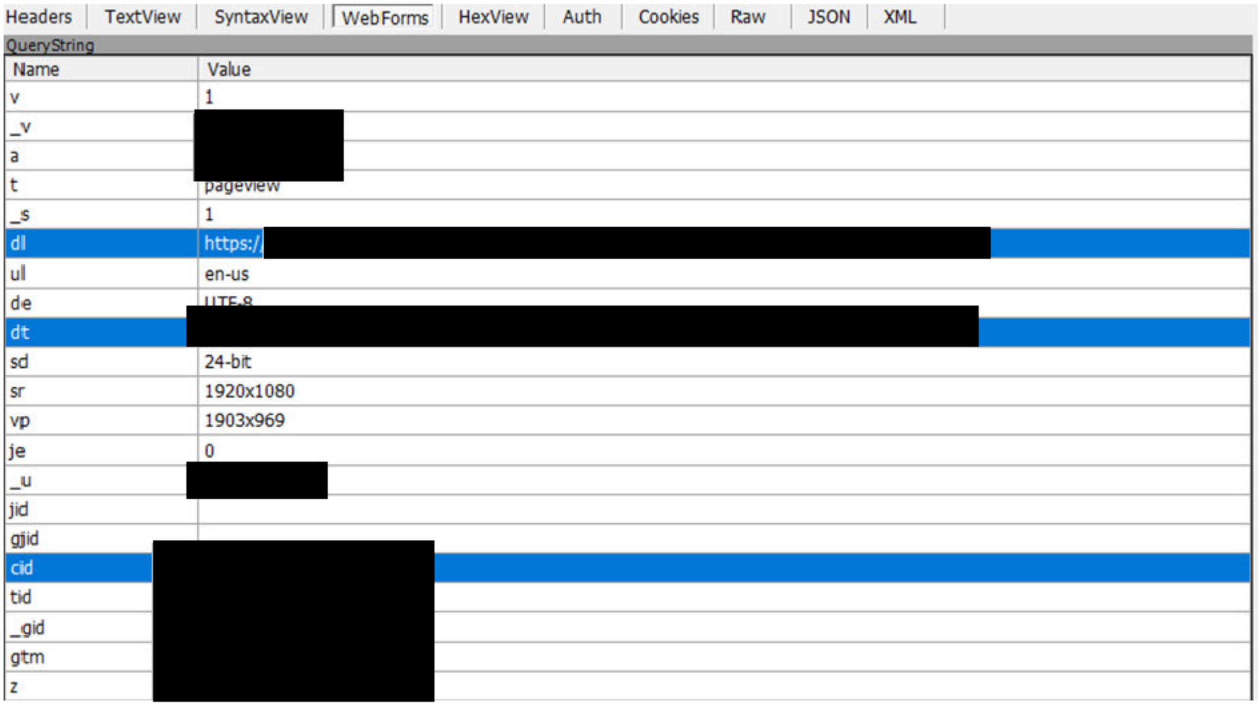


Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request Headers [Raw] [Header Definitions]

```
GET [redacted]
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.9
    User-
Cookies
⊟ Cook
      ID
Miscella
    Refer
    X-Clie
Security [redacted]
    Sec-Fetch-Dest: iframe
    Sec-Fetch-Mode: navigate
    Sec-Fetch-Site: cross-site
    Upgrade-Insecure-Requests: 1
Transport
    Connection: keep-alive
    Host: bid.g.doubleclick.net
```

192. And Chrome sent Kindler's personal information to Google Analytics:



Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

QueryString

Name	Value
v	1
_v	[redacted]
a	[redacted]
t	pageview
_s	1
dl	https:/[redacted]
ul	en-us
de	UTF-8
dt	[redacted]
sd	24-bit
sr	1920x1080
vp	1903x969
je	0
_u	[redacted]
jid	
gjid	[redacted]
cid	[redacted]
tid	[redacted]
_gid	[redacted]
gtm	[redacted]
z	[redacted]

193. Despite its promises to the contrary, Google combined Plaintiff Kindler's personal information that it obtained when she was not logged-in to Google Sync, including that she was a [redacted] patient who scheduled an appointment at [redacted] has an account at [redacted] and is taking continuing education courses on [redacted] Google combines this with other data is has

about her and will use that data to place Kindler in advertising categories from which Google will profit from targeted advertising to her based on data that it did not have the right to obtain.

H. Google's Improper Collection of PI from Plaintiffs and Other Un-Synched Chrome Users is a Serious Invasion of the Privacy and is Highly Offensive

194. Chrome is now the most widely used browser in the world and is used by 59 percent of all desktop computers in the United States.[19]

195. Article I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

196. The right to privacy in California's constitution creates a right of action against private as well as government entities.

197. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use and dissemination by public and private entities, including computer-stored and generated dossiers and cradle-to-grave profiles on every American.

198. In its public statements, Google pays lip-service to the need to protect the privacy of Internet communications. For example, On June 6, 2016, a coalition of technology companies and privacy advocates came together to oppose Congressional efforts to expand government surveillance of online activities through the Senate's Intelligence Authorization Act for Fiscal Year 2017 and Senator Cornyn's proposed amendments to the ECPA.

199. The joint letter, signed by the ACLU, Amnesty International and others ***was also signed by Google***. These organizations and companies argued (correctly) that obtaining sensitive information about Americans' online activities without court oversight was an unacceptable privacy harm because it "would paint an incredibly intimate picture of an individual's life" if it

[19] *Browser Market Share United States of America: May 2019 – May 2020*, GlobalStats, https://gs.statcounter.com/browser-market-share/all/united-states-of-america (last visited June 19, 2020).

included "browsing history, email metadata, location information, and the exact date and time a person signs in or out of a particular online account."

200. The letter further posited that the proposed online surveillance could "reveal details about a person's political affiliations, medical conditions, religion, substance abuse history, sexual orientation" and even physical movements. The letter concluded that online surveillance raises "civil liberties and human rights concerns."

201. Google has also publicly declared that non-consensual electronic surveillance is "dishonest" behavior. For example, earlier this month, Google announced an update to its "Enabling Dishonest Behavior Policy" (effective August 11, 2020) restricting advertising for spyware and surveillance technology. The new policy, without any hint of irony, will now "prohibit the promotion of products or services that are marketed or targeted with the express purpose of tracking or monitoring another person or their activities without their authorization."

202. Through this new amendment to Google's pre-existing policy, Google now explicitly takes the position that nonconsensual surveillance of "browsing history" is "dishonest behavior."

203. Google has also publicly declared privacy to be a human right. In 2004 in a letter from Google's founders to shareholders at the IPO (included with the Company's S-1 Registration Statement filed with the SEC), Google declared its goal to "improve the lives of as many people as possible." This letter appears today on Google's website on a page touting the company's commitment to be guided by "internationally recognized human rights standards," including specifically the human rights enumerated in three documents: The Universal Declaration of Human Rights; the United Nations Guiding Principles on Business and Human Rights; and the Global Network Initiative ("GNI") Principles.

204. All three of these documents confirm that privacy is a human right and a violation of privacy rights is a violation of human rights.

205. For example, the Universal Declaration declares that no one should be subject to arbitrary interference with privacy, and even declares the right to the protection of laws against such interference.

206. Similarly, the UN Guiding Principles for business identify privacy as a human right.

207. The third document, the GNI Principles, has an entire section dedicated to privacy that begins: “Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.”

208. Finally, although not mentioned on Google’s website, in 1992 the United States ratified the International Covenant on Civil and Political Rights, a human rights treaty that guarantees privacy rights in Article 17.

I. Plaintiffs’ PI Is Property Owned by the Plaintiffs and Has Economic Value

209. The value of personal data is well understood and generally accepted as a form of currency.

210. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

211. The robust market for user data has been analogized to the “oil” of the tech industry.[20] A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge.”[21] That article noted that the value of a single Internet user—or really, a single user’s data—varied from about $15 to more than $40.

212. The Organization for Economic Cooperation and Development (“OECD”) itself has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication “Exploring the Economic of

[20] *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[21] Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?* TechCrunch (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

Personal Data: A Survey of Methodologies for Measuring Monetary Value".[22] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[23]

213. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes Google's early success monetizing user data prompted large corporations like Verizon, AT&T and Comcast to transform their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[24] In essence, Professor Zuboff explains that revenue from user data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a ***market*** for this data; data generated by users on Google's platform has economic value.

214. This is old news. In 2012, Google's Chief Economist Hal Varian, in conversation with the *Economist*, referred to one aspect of data's value as "nowcasting," or "contemporaneous forecasting"—basically an ability to predict what is happening as it actually occurs."[25] This kind of information clearly has economic value.

215. Professor Paul M. Schwartz writing in the Harvard Law Review, notes:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

[22] *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en.

[23] *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

[24] Shoshanna Zuboff, The Age of Surveillance Capitalism 166 (2019).

[25] K.N.C., *Questioning the searches*, The Economist (June 13, 2012), https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers.

216. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[26] Google itself has launched apps that pay users for their data directly.[27] Likewise, apps such as Zynn, a TikTok competitor, pay users for to sign up and interact with the app.[28]

217. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

218. Indeed, Google once paid users for the very data it now improperly harvests from Chrome:

> Google is building an opt-in user panel that will track and analyze people's online behaviors via an extension to its Chrome browser, called Screenwise. Users that install the plug-in will have the websites they visit and the ways in which they interact with them recorded, and they will then be paid with Amazon gift cards worth up to $25 a year in return.[29]

219. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article "The Economics of Privacy," published in the *Journal of Economic Literature*:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's

[26] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[27] Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019), https://www.theguardian.com/technology/2019/jun/11/Google-user-data-app-privacy-study; Saheli Roy Choudhury and Ryan Browne, *Google pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/Google-paying-users-to-install-app-to-collect-data-techcrunch.html; Tim Bradshaw, *Google offers to pay users for their voice recordings*, Financial Times (Feb. 21, 2020), https://www.ft.com/content/42f6b93c-54a4-11ea-8841-482eed0038b1.

[28] Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival.

[29] Jack Marshall, *Google Pays Users for Browsing Data*, DigiDay (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/.

> age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[30]

220. There also a private market for users' personal information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for $1,200 on the dark web.[31] These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users can sell their own. In short, there is economic value to users' data that is greater than zero. The exact number will be a matter for experts to determine.

J. Plaintiffs Have Suffered Economic Injury

221. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

222. Personal Information, including websites visited by the Plaintiffs, is property under California law.

223. Property includes intangible data, including the very specific data at issue here that Google is taking despite promising users that it would not do so—personal information including Internet communications history and personally identifiable information.

224. Taking Plaintiffs' PI without authorization is larceny under California law regardless of whether and to what extent Google monetized the data, and Plaintiffs have a right to disgorgement and/or restitution damages for the value of the stolen data.

225. Plaintiffs also have suffered benefit of the bargain damages, in that Google took more data than the parties agreed would be exchanged. Those benefit of the bargain damages also

[30] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf.

[31] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MarketWatch (June 6, 2018), https://www.marketwatch.com/story/spooked-by-the-Google-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20.

include, but are not limited to, (i) loss of the promised benefits of their Chrome experience; (ii) out-of-pocket costs; and (iii) loss of control over property which has marketable value.

226. In addition, when Plaintiffs became Chrome users, they gained access to Chrome's browser in exchange for agreeing to terms of service that Chrome drafted and sharing a limited amount of data reflecting users' activity on the platform. In other words, those terms of service assured users that data would not be sent to Google which was intended to, and did, encourage Plaintiffs to engage more than they would have otherwise. The delta in data between what Chrome promised and what in fact Chrome sent to Google can be measured in data and also in dollars, because data has value.

227. Data brokers and online marketers have developed sophisticated schemes for assessing the value of certain kinds of data, as discussed above. Experts in the field have identified specific values to assign to certain kinds of activity. While Plaintiffs largely knew that Google generates revenue from business by selling advertising directed at users, it was a material term of the bargain that Plaintiffs' personal information would not be shared with Google if users did not take the affirmative step of activating Sync for their Chrome account. It was also a material term of the bargain that user would not "need to provide any personal information to use Chrome."

228. Google did not honor the terms of this bargain. Although the Chrome Privacy Notice stated that Plaintiffs' did not "need to provide any personal information to use Chrome" and that their personal information would not be shared with Google unless they Sync'd their account, in practice, their information was shared with Google as if they had activated Sync.

229. When Chrome shared and Google collected Plaintiffs' personal information from Chrome that Plaintiffs had not chosen to share with Google, Google received benefits. First, Google captured-revenues associated with increased user activity on the Chrome browser and from enhanced targeting as a result of ever-more detailed datasets collected about users. Second, Google also transferred costs and harms to Plaintiffs in that Google did not have to invest in protecting that data or preventing its dissemination as it promised users it would.

230. As Google expanded the scope of access to Plaintiffs' personal information beyond that which Plaintiffs had agreed, users were denied the benefit of a Chrome experience where they

were promised the right to determine the terms and scope of their content and personal information sharing. Thus, through Chrome's sharing of Plaintiffs' personal information with Google, Plaintiffs lost benefits.

231. In order to preserve their privacy, Plaintiffs who now understand at least some of Google's violations—and there is much to be revealed about Google's actual activities—are presented with the choice of: (i) reducing or ending their participation on Chrome; or (ii) knowingly accepting less privacy than that which was promised. Each of these options deprives Plaintiffs of the remaining benefits of their original bargain. There is no option which recovers it. None of it recaptures the data taken in violation of Chrome's promises.

232. Further, Plaintiffs were denied the benefit of this information and therefore the ability to mitigate harms they incurred because of Chrome's impermissible disclosure of their personal information to Google. That is, Google's lack of transparency prevented and still prevents Plaintiffs' ability to mitigate.

233. Google knew that it was collecting users' personal information regardless of whether users had taken affirmative steps to turn on the synchronization feature. Yet, Google failed to warn users so that they could take steps to avoid exposing their information on Chrome.

234. Google also knew that it was not possible for users to use Chrome without providing any personal information.

235. Google avoided costs it should have incurred because of its own actions—particularly the loss of user engagement which would have resulted from transparent disclosure of Googler's actions—and transferred those costs to Plaintiffs. Warning users would have chilled Chrome engagement as well as discourage potential new users from joining.

236. Google was thus not only able to evade or defer these costs but to continue to accrue value for the Company and to further benefit from the delay due to the time value of money. Google has thus transferred all the costs imposed by the unauthorized disclosure users' content and personal information onto Plaintiffs. Google's increased mitigation costs by failing to notify users that their personal information had been disclosed and to alert them at the earliest time possible so that users could take steps to minimize their exposure on the browser.

237. In addition, Plaintiffs have also suffered from the diminished loss of use of their own personal information, property which has both personal and economic value to them.

238. Plaintiffs' personal information has value. First, there is transactional, or barter, value to user content and personal information. Indeed, Google has traded the ability to use its Chrome browser for the collection of users' personal information—all the while promising users that it was not necessary for them to share any personal information to use Chrome and that Chrome would not share any of their personal information with Google unless they were Synched.

239. Second, Plaintiffs' property, which has economic value, was taken from them without their consent and in contradiction of Chrome's express promise not to send it to Google. There is a market for this data, and it has at minimum a value greater than zero.

240. Users were harmed when Google took their property and exerted exclusive control over it, collecting it without users' knowledge and for still undisclosed purposes.

K. Google Has Been Unjustly Enriched

241. Google's $1 trillion business was built entirely on monetizing the value of Internet users' data.[32]

242. Professor Zuboff details Google's role as one of the main drivers of data collection and monetization:

> In 2016, 89 percent of the revenues of [Google's] parent company, Alphabet, derived from Google's targeted advertising programs. The scale of raw-material flows is reflected in Google's domination of the internet, processing over 40,000 search queries every second on average: more than 3.5 billion searches per day and 1.2 trillion searches per year worldwide in 2017.[33]

243. Indeed, "Google maximizes the revenue it gets from [landing pages] by giving its best position to the advertiser who is likely to pay Google the most in total, based on the price per

[32] *Google owner Alphabet is now worth $1 trillion*, CNN (Jan. 16, 2020), https://www.cnn.com/2020/01/16/investing/google-trillion-dollar-market-value-apple-microsoft/index.html.

[33] Zuboff, *supra*, at 92

click multiplied by Google's estimate of the likelihood that someone will actually clock on the ad."[34]

244. For its part, Google explains under the header of "How we make money" in its annual financial statements, that its goal is to "deliver relevant ads at just the right time and to give people useful commercial information, regardless of the device they're using."[35] Google explains further that it revenues are based primarily on the delivery of "performance advertising," and "brand advertising."

245. Performance advertising, as Google explains, is driven by users' engagement with an advertisement and Google is paid by the advertiser when a user engages in the ad. Brand advertising is built through "enhance[ing] users' awareness of and affinity with advertisers' products and services, through videos, text, images, and other interactive ads that run across various devices." Under both, Google's revenues are built upon the ability to target users with advertisements based upon the personal information that Google has collected.

246. The value of Chrome users' personal information to Google is demonstrated in part by Google's advertisement revenue during the relevant time period. Google reported $134.8 billion in advertising revenue in 2019, $116.4 billion in 2018, $95.5 billion in 2017, and $79.3 billion in 2016.[36] This translates to 83% of Google's total revenues in 2019, 85% in 2018, 86% in 2017 and 87% in 2016.[37] While not all of that value is unjustly derived from the specific information collected by Google here, some portion of it is.

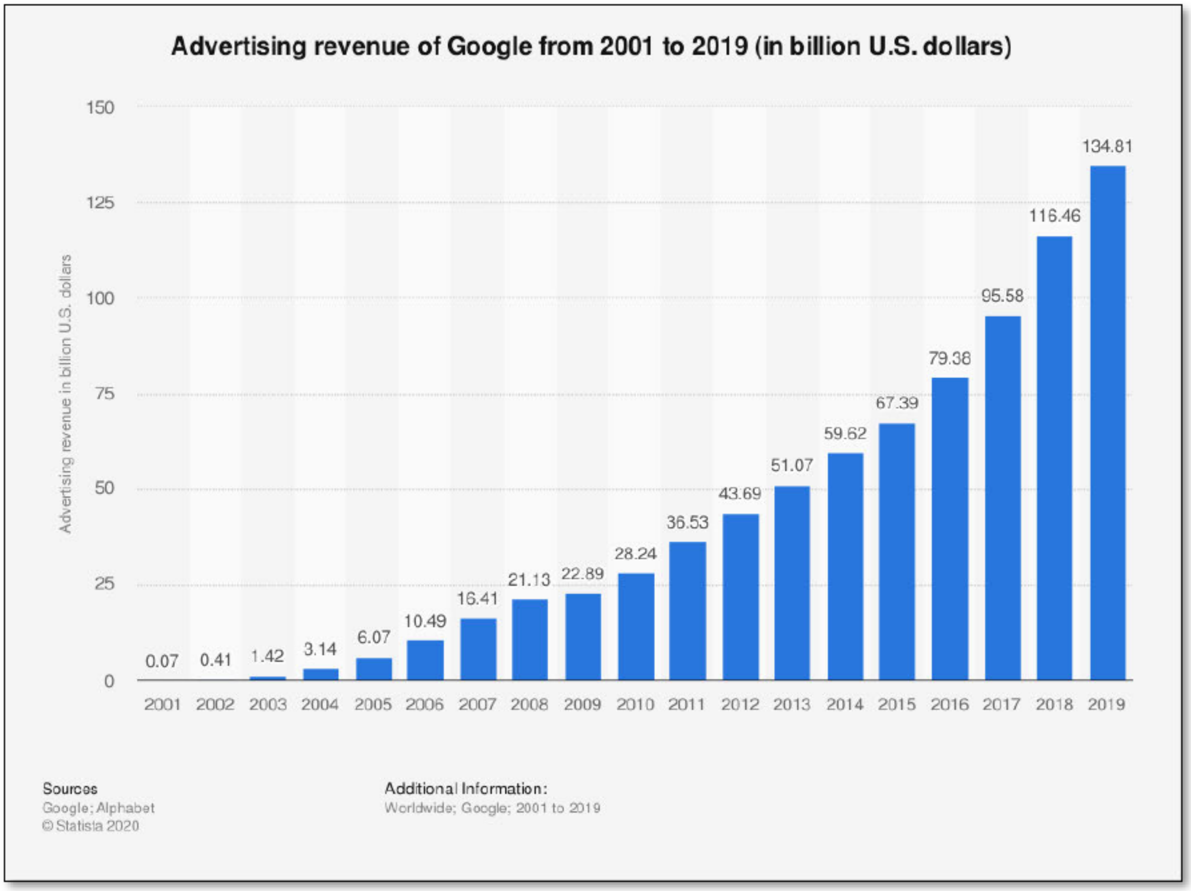
[34] Peter Coy, *The Secret to Google's Success*, Bloomberg (Mar. 6, 2006), http://www.bloomberg.com/news/articles/2006-03-05/the-secret-to-googles-success.

[35] *2019 Annual Report*, Alphabet Inc. (Feb. 3, 2020), https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#sFA530FF828B154C8973614936FC32E93.

[36] *2019 Annual Report*, Alphabet Inc. (Feb. 3, 2020), https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#sFA530FF828B154C8973614936FC32E93; *2018 Annual Report*, Alphabet Inc. (Feb. 4, 2019), https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm.

[37] 2019 Annual Report; 2018 Annual Report.

247. Shown graphically below, Google's annual advertising revenue has increased over five hundred percent since it first released Chrome in 2008.[38]


Advertising revenue of Google from 2001 to 2019 (in billion U.S. dollars)

Sources
Google; Alphabet
© Statista 2020

Additional Information:
Worldwide; Google; 2001 to 2019

248. Google's increased revenue is driven in part by the increased engagement by users, which Google quantifies as "paid clicks" across Google properties, including Chrome. According to Google's annual reports, Google has increased the number of its paid clicks by 23% in 2019, 62% in 2018, 70.5% in 2017, and 70.9% in 2016.

249. In addition to these metrics, estimates of Google average revenue per monthly active user from advertising on its sites is $6.70 in the fourth quarter of 2016.[39] Other estimates of the

[38] J. Clement, *Advertising revenue of Google from 2001 to 2019*, statista (Feb. 5, 2020), https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

[39] J. Clement, *Google's average revenue per monthly active user from 1st quarter 2015 to 4th quarter 2016* , statista (May 24, 2017), https://www.statista.com/statistics/306570/google-annualized-advertising-arpu/.

average revenue per user per year for Google place the value at $256.[40] And at $55 for digital revenue per member.[41]

250. The collection of users' PI has also facilitated the revenues of Google's Network Members' properties which include ads placed through AdMob, AdSense, DoubleClick AdExchange. Google's Network Members' properties revenues increased by $21.5 in 2019, $20 billion in 2018, $17.6 billion in 2017, and $15.5 billion in 2016.[42]

251. Google uses information collected from users to deliver targeted advertisements to users across Google's services and across users' devices. The delivery of targeted advertisements leads to more engagement with the advertisements, which allows Google to sell the advertisements at a higher rate.

252. Google has recently disclosed the shared take rates from buying portals, Google Ads and Display & Video 260, and from publisher services, Google Ad Manager. The disclosure show that "when marketers used Google Ads or Display & Video 360 to buy display ads on Google Ad Manager," Google keeps 31% of the ad spend.[43] Google's cut of the ad spend further demonstrates the markup achieved by its collection, and use of users' personal information.

253. Google further quantifies the value of users' data through several user-based metrics, including cost-per-impressions and cost-per-click. Google defines "cost-per-impressions" for Google Network Members' properties, such as AdMob, AdSense, DoubleClick AdExchange, as the "impression-based and click-based revenues divided by our total number of impressions and

[40] Frederic Filloux, *The ARPUs of the Big Four Dward Everybody Else*, Medium (Feb. 10, 2019), https://mondaynote.com/the-arpus-of-the-big-four-dwarf-everybody-else-e5b02a579ed3.

[41] Fredric Filloux, *The NYTimes could be worth $19bn instead of $2bn*, Medium (Feb. 15, 2015), https://mondaynote.com/the-nytimes-could-be-worth-19bn-instead-of-2bn-8ab635bc6262.

[42] 2019 Annual Report; 2018 Annual Report.

[43] Sissie Hsiao, *How our display buying platforms share revenue with publishers*, Google Ad Manager (June 23, 2020), https://blog.google/products/admanager/display-buying-share-revenue-publishers/.

represents the average amount we charge advertisers for each impression displayed to users."[44] Google reported a 9% increase in cost-per-impressions for 2019, and 2% increase in 2018.

254. Google also reports the "cost-per-click," which it defines as "click-driven revenues divided by our total number of paid clicks and represents the average amount we charge advertisers for each engagement by users."[45] Google does not include the actual cost-per-click in financial reports. However, the average costs per click on Google Ads is reportedly $2.32.[46]

255. Google's user-based revenues are driven by its collection of Internet users' information to create detailed dossiers about individual's personal information, including names, address, education, income, hobbies, interests, relationships, politics, religious beliefs, and more.

256. Although Google promises that Chrome users can opt out of Google surveillance by not providing any personal information to use Chrome and not Synching their data, those promises are not true. And Chrome plays a large part, with over 2 billion active installs allowing data generation and extraction trillions of times on a daily basis.[47]

257. Unbeknownst to users, Google has programmed Chrome for surveillance no matter what the user does. By encouraging engagement with Chrome with its promise not to share data with Google, Google ensures that it will be able to track an ever-larger percentage of Internet users.

258. In other words, Chrome's promise not to send Un-Synched users' PI to Google was intended to (and did) stimulate greater user engagement. Those false promises also prevented decreased user engagement by disclosing what Chrome's actual practices are. And Google directly profited from that increased user engagement.

[44] 2019 Annual Report.

[45] *Id.*

[46] Dan Shewan, *The Comprehensive Guide to Online Advertising Costs*, WordStream (Apr. 20, 2020), https://www.wordstream.com/blog/ws/2017/07/05/online-advertising-costs#:~:text=The%20average%20cost%20of%20an,18..

[47] Frederic Lardinois, *Google says there are now 2 billion active Chrome installs*, TechCrunch (Nov. 10, 2016), https://techcrunch.com/2016/11/10/google-says-there-are-now-2-billion-active-chrome-installs/.

VI. CLASS ACTION ALLEGATIONS

259. This is a class action pursuant to Rules 23(a) and (b)(3) (or, alternatively, 23(c)(4)) of the Federal Rules of Civil Procedure on behalf of a Class of all persons residing in the United States who used Google's Chrome browser on or after July 27, 2016 without choosing to Sync with any Google account and whose personal information was collected by Google.

260. Excluded from the Class are the Court, Defendants and their officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

261. The members of the Class are so numerous that joinder of all members is impracticable.

262. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class include:

a. Whether Chrome shares user personal information with Google when users were not Synched with their Google accounts;

b. Whether Chrome users can use the service without providing personal information to Chrome;

c. Whether Google had authorization from Un-Synched Chrome Users to disclose the content of user communications while in storage on the Chrome browser;

d. Whether Google had user authorization from Un-Synched Chrome Users to disclose the content of user communications contemporaneous to their making;

e. Whether Google had user authorization from Un-Synched Chrome Users to acquire the content of user communications while they were in storage in the Chrome browser;

f. Whether Google had user authorization from Un-Synched Chrome Users to acquire the content of user communications contemporaneous to their making;

g. Whether Google's actions to disclose and acquire the contents of Un-Synched Chrome User communications violate the federal Electronic Communications Privacy Act;

h. Whether Google's actions violate the California Invasion of Privacy Act;

i. Whether Google breached its contract with Un-Synched Chrome Users;

j. Whether the Personal Information improperly collected by Google from the Un-Synched Users has economic value; and

k. Whether Google unjustly profited from the improperly collected Personal Information of the Un-Synched Chrome Users.

263. Plaintiffs' claims are typical of the claims of other Class members, as all members of the Class were similarly affected by Google's wrongful conduct in violation of federal and California law as complained of herein.

264. Plaintiffs will fairly and adequately protect the interests of the members of the Class and have retained counsel that is competent and experienced in class action litigation. Plaintiffs have no interest that conflict with, or is otherwise antagonistic to the interests of, the other Class members.

265. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages individual Class and Subclass members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class and Subclass to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

VII. COUNTS

COUNT ONE

WIRETAP ACT: UNAUTHORIZED INTERCEPTION OF ELECTRONIC COMMUNICATIONS 18 U.S.C. § 2510, *et seq.*

266. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

267. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

268. The ECPA protects both the sending and receipt of communications.

269. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

270. Google intentionally intercepted the electronic communications of Plaintiffs and other Un-Synched Chrome Users.

271. The transmission of data between plaintiffs and the websites on which Google tracked and intercepted their communications without authorization while they were Un-Synched were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

272. Google's interception of Plaintiffs' communications was done contemporaneously with the Plaintiffs' sending and receipt of those communications.

273. The intercepted communications include:

a. The precise text of GET requests that Chrome users' exchange with non-Google websites;

b. The precise text of user search queries at non-Google sites;

c. The precise text of specific buttons that users click to exchange communications at non-Google websites, such as "Log-In" or "Submit."

d. The precise text of information that users submit in forms to exchange communications at non-Google websites.

e. Information that is a general summary or informs Google of the general subject of communications that non-Google websites send back to users in response to search queries and requests for information.

274. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Google used to track the Plaintiffs' communications while they were not Synched with any Google account, including cookies Google sets and acquires through other entities through cookie-synching;

b. The Plaintiffs' browsers;

c. The Plaintiffs' computing devices;

d. Google's web servers;

e. The web-servers of websites from which Google tracked and intercepted the Plaintiffs' communications while they were not Synched with any Google account; and

f. The computer code deployed by Google to effectuate its tracking and interception of the Plaintiffs' communications while not Synched with any Google account.

275. Google is not a party to Plaintiffs' electronic communications with non-Google websites.

276. Google's received the content of Plaintiff communications with non-Google websites through the surreptitious duplication and forwarding of those communications by Chrome to Google.

277. Plaintiffs were logged-off of Google Sync when Google intercepted the communications at issue.

278. Plaintiffs did not consent to Google's acquisition of the contents of their communications with non-Google websites while using the Chrome browser when not logged-in to Google Sync because Google expressly promised that "[t]he personal information that Chrome stores [about users] won't be sent to Google unless" the Chrome user "choose[s] to store that data

Case 5:20-cv-05146 Document 1 Filed 07/27/20 Page 72 of 93

in" their "Google Account by turning on sync," i.e. formally logging-in to a Google service called Sync.

279. Google's failure to adequately inform websites using its third-party tracking tools that Google had promised Chrome users that it would not share user personal information unless the user was logged-in to Sync constituted a fraud and mistake of fact that vitiates any alleged consent that Google may claim for the non-Google websites.

280. The ECPA includes a separate affirmative defense for the officers, employees, and agents of electronic communication service providers, whose facilities are used in the transmission of electronic communications, "to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or the protection of the rights or property of the provider of that service[.]"

281. As alleged herein, the Google services to which Chrome re-directs Chrome user communications are not agents of Chrome.

282. The surreptitious re-direction of Chrome user communications to Google while the users were not logged-in to Google Sync was not done in Chrome's "normal course" and is not a "necessary incident to the rendition" of electronic communication service.

283. The surreptitious re-direction of Chrome user communications to Google while users were not logged-in to Google Sync was not done for "the protection of the rights or property" of Chrome, but instead for advertising and surveillance purposes by Google's other services.

284. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT TWO

WIRETAP ACT – UNAUTHORIZED DISCLOSURES BY AN ECS 18 U.S.C. § 2510, *et. seq.*

285. The Electronic Communications Privacy Act provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

286. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

287. Google Chrome is an ECS because it provides to users thereof the ability to send or receive electronic communications.

288. In the absence of a web-browser, Internet users could not send or receive communications over the Internet.

289. Chrome is an ECS provided to the public.

290. Chrome intentionally divulged the contents of user communications with non-Google websites to Google while those user communications were in transmission on Chrome.

291. Google was not an addressee or intended recipient of Plaintiffs' communications on Chrome while they were not logged-in to Google Sync.

292. Google was not an addressee or intended recipient of the non-Google websites communications to Plaintiffs' using Chrome while they were not logged-in to Google Sync.

293. Google was not an agent of the Plaintiffs or the non-Google websites.

294. The ECPA provides that "a person or entity providing an [ECS] to the public may divulge the contents of any such communication—(i) as otherwise authorized in sections 2511(2)(a) or 2517 of this title;" (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are

used, to forward such communication to its destination; (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

295. Section 2511(2)(a) exempts the contents of communications divulged to "an officer, employee, or agent" of an ECS "in the normal course of employment … while engaged in any activity which is a necessary incident to the rendition" of service "or to the protection of the rights or property of the provider of that service[.]" Google lacks this affirmative defense because Chrome's divulgences to Google Doubleclick, Google Analytics, Google Ads, and other Google divisions was not "in the normal course" of the provision of ECS, was not a "necessary incident to the rendition" of ECS service, and was not for "the protection of the rights or property" of Google. Instead, the divulgences were for Google's advertising and surveillance purposes.

296. Section 2517 relates to divulgences to law enforcement officers and is not pertinent here.

297. Chrome lacks the "lawful consent" of the originator and any addressee or intended recipients of the relevant communications because:

a. Chrome expressly promised its ECS users that their personal information, including the contents of their browsing communications, would not be shared with Google unless the user was logged-in to Google Sync;

b. Chrome and Google failed to inform non-Google websites using Google third-party tracking source code that Chrome promised its users not to divulge such information; and

c. Chrome failed to block divulgences of Chrome user communications to Google advertising entities when users were not logged-in to Google Sync, despite having promised to not share such information with Google in those circumstances.

298. The Google advertising entities to which the contents of Chrome users' communications were divulged are not employed or authorized, and do not have facilities used, to forward user communications to their intended destinations.

299. The affirmative defines for disclosures to law enforcement does not apply.

300. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT THREE

STORED COMMUNICATIONS ACT – UNAUTHORIZED ACCESS TO STORED ECS COMMUNICATIONS 18 U.S.C. § 2701

301. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

302. The Stored Communications Act ("SCA") provides a cause of action against a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

303. As set forth above, Google Chrome is an ECS. Google has explained that a web browser is where Internet users "search, chat, email, and collaborate," and, "in our spare time, we shop, bank, read news, and keep in touch with friends – all using a browser."

304. The ECPA does not provide a separate definition for "facility" but instead it is defined within the context of the sentences in which it is used.

305. A "facility" under the ECPA is, under the plain language of the statute, that "through which an electronic communication service is provided." 18 U.S.C. § 2701(a).

306. The ECPA also uses the term "facility" when describing the facts necessary to support a law enforcement application for a Wiretap order, which "shall include," among other things "a particular description of the nature and location of the facilities from which or the pace where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b). As used in this ECPA

section, “facility” has included telephones and other communications devices that officers have formally requested to be tapped.

307. The items through which the electronic communication services of the Chrome web-browser include:

a. The Plaintiffs’ personal computing devices;

b. The Plaintiffs’ Chrome browsers;

c. The browser-managed files which, together, constitute all of the programs contained within the Plaintiffs’ Chrome browsers; and

d. Plaintiffs’ IP addresses.

308. Google intentionally accessed the Plaintiffs’ personal computing devices, Chrome browsers, browser-managed files, and IP addresses via the Chrome browser while the Plaintiffs were not logged-in to Google Sync.

309. Plaintiffs did not authorize Google to access the content of their communications stored on their personal computers and the Chrome browser while they were not logged-in to Google Sync.

310. The information obtained by Google through its unauthorized access included “contents” as described above

311. The ECPA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

312. Chrome stores the contents of user communications immediately upon a user’s sending of any communication in at least two ways:

a. For purposes of backup protection so that if the browser inadvertently shuts down, the user can be presented with the option to restore previous communications; and

b. For a temporary and intermediate amount of time incidental to the electronic transmission thereof when it places the contents of user

> communications into the browser's web-browsing history, which is only kept on the browser for 90 days.

313. Plaintiffs and Class Members were harmed by Google's actions, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Google attributable to the violations or statutory minimum damages of $1,000 per plaintiff, punitive damages, costs, and reasonable attorney's fees.

COUNT FOUR

STORED COMMUNICATIONS ACT – UNAUTHORIZED DISCLOSURES OF STORED COMMUNICATIONS BY AN ECS 18 U.S.C. § 2701

314. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

315. The ECPA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."

316. As alleged above, Google Chrome is an ECS to the public.

317. As alleged above, Chrome knowingly divulges the contents of user communications to Google while those user communications are in electronic storage by Chrome.

318. Plaintiffs and Class Members were harmed by Google's actions, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Google attributable to the violations or statutory minimum damages of $1,000 per plaintiff, punitive damages, costs, and reasonable attorney's fees.

COUNT FIVE

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA") Cal. Penal Code §§ 631

319. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

320. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and

> techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

321. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner ….willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars …

322. Google is a "person" or "persons" within the meaning of § 631(a).

323. Under § 631, a defendant must show it had the consent of all parties to a communication.

324. Google is headquartered in California; designed and contrived and effectuated its scheme to track its users while not logged-in to Sync in California; and has adopted California substantive law to govern its relationship with its users.

325. At all relevant times, Google's tracking and interceptions of the Plaintiffs' Internet communications while not logged-in to Sync was without authorization and consent from the Plaintiffs.

326. Google's non-consensual tracking of logged-out users' Internet browsing was designed to learn or attempt to learn the meaning of the contents of Chrome users' communications.

327. Chrome aided and abetted Google in its learning or attempting to learn the meaning of the contents of Chrome users' communications.

328. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The cookies Google used to track the Plaintiffs' communications while they were not logged-in to Google Sync;

b. The Plaintiffs' browsers;

c. The Plaintiffs' personal computing devices;

d. Google's web servers;

e. The web-servers of non-Google websites from which Google tracked and intercepted the Plaintiffs' communications while they were not logged-in to Google Sync; and

f. The computer code Google deployed to effectuate its tracking and interception of the Plaintiffs' communications while Plaintiffs were not logged-in to Google Sync;

g. The plan Google carried out to achieve its tracking and interception of the Plaintiffs' communications while they were not logged-in to Google Sync.

329. Google's learning or attempts to learn the contents of Plaintiffs' communications while not logged-in to Google Sync occurred while Plaintiffs' communications with non-Google websites were in transit or in the process of being sent or received.

330. Plaintiffs and Class Members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their PI.

331. Pursuant to Cal. Pen. Code § 637.2, Plaintiffs and the Class have been injured by Defendant's violations of Cal. Pen. Code § 631 and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT SIX

INVASION OF PRIVACY

332. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

333. Google has intruded upon the following legally protected privacy interests of Plaintiffs:

a. A right to privacy contained on personal computing devices, including web-browsing history;

b. A right to be free from Internet surveillance absent consent;

c. Statutory rights codified in federal and California privacy statutes;

d. The California Computer Crime Law, Cal Pen. Code § 502, which applies to all plaintiffs in this case by virtue of Google's choice of California law to govern its relationship with Google users;

e. Cal. Penal Code § 484(a) which prohibiting the knowing theft or defrauding of property "by any false or fraudulent representation or pretense[.]"

334. The Google Terms of Service, and other public promises Google made not to track or intercept the Plaintiffs' communications or access their computing devices and Chrome browsers while not Synched with any Google accounts.

335. Plaintiffs had a reasonable expectation of privacy in the circumstances in that:

a. Plaintiffs could not reasonably expect Google would commit acts in violation of federal and state laws;

b. Google affirmatively promised users it would not cause Chrome to send their personal information to Google unless the users choose to Sync with their Google accounts

336. Google's actions constituted a serious invasion of privacy in that they:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search and browsing histories;

b. Violated several federal criminal laws, including the Wiretap Act, and Stored Communications Act;

c. Violated dozens of state criminal laws;

d. Invaded the privacy rights of hundreds of millions of Americans without their consent;

e. Constituted the unauthorized taking of valuable information from hundreds of millions of Americans through deceit.

337. The surreptitious and unauthorized tracking of the internet communications and associated personal information of millions of Americans' constitutes an egregious breach of social norms.

338. Google lacked a legitimate business interest in tracking users without consent.

339. Plaintiffs have been damaged by Google's invasion of their privacy and are entitled to just compensation.

COUNT SEVEN

INTRUSION UPON SECLUSION

340. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

341. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

342. In carrying out its scheme to track and intercept Plaintiffs' communications and access their computing devices and Chrome browsers while they were not Synched with other Google accounts in violation of the governing Terms of Service, Google intentionally intruded upon the Plaintiffs' solitude or seclusion in that it effectively placed itself in the middle of communications to which it was not an authorized party and acquired data that was private and Google was not authorized to acquire.

343. Google's actions were not authorized by the Plaintiffs nor by the websites with which they were communicating.

344. Defendant's intentional intrusion into Plaintiffs' Internet communications and their computing devices and Chrome browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

345. The unauthorized disclosure and taking of personal information from hundreds of millions of Americans through deceit is highly offensive behavior.

346. Secret monitoring of web browsing is highly offensive behavior.

347. Wiretapping and surreptitious recording of communications is highly offensive behavior.

348. Public polling on Internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]."[48]

349. Plaintiffs have been damaged by Google's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

COUNT EIGHT

BREACH OF CONTRACT

350. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

351. Google's relationship with its users is governed by the Google general Terms of Service, Chrome TOS and Chrome Privacy Notice, current and prior versions of which are attached to this Complaint as Exhibits 2 through 33.

352. Google promised that Chrome would not report PI to Google unless the Plaintiffs affirmatively chose to Sync the browser with their Google accounts.

353. Google breached this promise.

354. Plaintiffs fulfilled their obligations under the relevant contracts and are not in breach of any.

355. As a result of Google's breach, Google was able to obtain the personal property of Plaintiffs and other Un-Synched Chrome Users, earn unjust profits, and caused privacy injury and other consequential damages.

[48] Auxier and Rainie, "Key takeaways on Americans' views about privacy, surveillance and data-sharing" https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ (last accessed July 23, 2020).

356. Plaintiffs and other Un-Synched Chrome Users also did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of the PI they agreed to share, which, as alleged above, has ascertainable value to be proven at trial.

COUNT NINE

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

357. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

358. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement.

359. In dealing between Google and its users, Google is invested with discretionary power affecting the rights of its users.

360. Google purports to respect and protect its users' privacy.

361. Despite its contractual privacy promises not to track users who choose not to Sync Chrome with other Google accounts, Google took actions outside those contractual promises to deprive Plaintiffs and the class of the benefits of their contract with Google.

362. Google's tracking and interception of the Internet communications and access to the computing devices and Chrome browsers of logged-off users was objectively unreasonable given Google's privacy promises.

363. Chrome's unauthorized disclosures of users' personal information to Google was objectively unreasonable given Chrome's privacy promises.

364. Google's conduct in tracking and intercepting the Internet communications and accessing the computing devices and Chrome browsers of logged-off users evaded the spirit of the bargain made between Google and the plaintiffs.

365. Google's conduct in this case abused its power to specify terms—in particular, Google's failed to accurately disclose its tracking of users while they were logged-off of Google Sync.

366. As a result of Google's misconduct and breach of its duty of good faith and fair dealing, Plaintiffs and the Class suffered damages. Plaintiffs and the Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration

in the form of their personal information, which, as alleged above, has ascertainable value to be proven at trial.

COUNT TEN

QUASI-CONTRACT (RESTITUTION AND UNJUST ENRICHMENT)
(IN ALTERNATIVE TO CONTRACT CLAIMS)

367. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

368. Defendant, intentionally and without consent or other legal justification, violated the privacy, property, and statutory rights of Plaintiffs and other Un-Synched Chrome Users.

369. As a result of Defendant's tortious acts, Defendant received and unjustly retained a benefit at the expense of Plaintiffs and other Un-Synched Chrome Users.

370. It would be unjust for Defendant to retain the value of the Plaintiffs' property and any profits earned thereon.

371. If Plaintiffs' contract claims fail they have no adequate remedy at law to force the disgorgement of Defendant's unjustly earned profits. This count is therefore pled in the alternative to the contract claims.

COUNT ELEVEN

VIOLATION OF COMPUTER FRAUD AND ABUSE ACT ("CFAA")
18 U.S.C. §1030(g)

372. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

373. The CFAA prohibits the knowing "transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A).

374. The Plaintiffs' computers are "protected computers" within the meaning of the statute.

375. The Chrome browser was represented to protect user privacy (by blocking the transmission of PI to Google) unless the user affirmatively elected to Sync the browser with other Google accounts.

376. Chrome's purported ability to protect user privacy was a core feature of Chrome.

377. Google transmitted code to the Plaintiffs' computers that caused Chrome to transmit PI to Google without Plaintiff's authorization.

378. The CFAA defines "damage" to mean "impairment to the integrity or availability of data, a program, a system or information."

379. Google's unauthorized actions impaired the integrity of Plaintiffs' data, browsers and computer systems by removing a key privacy feature that should have blocked Google's surveillance.

380. The CFAA provides a private right of action by any person who suffers damage or loss as a result of Defendant's unauthorized actions.

381. Plaintiffs seek money damages and injunctive relief as provided under the statute.

COUNT TWELVE

VIOLATION OF CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT
Cal. Penal Code § 502

382. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

383. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information.

384. Defendant accessed, copied, used, made use of, interfered with, and/or altered data belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the states in which the Plaintiffs and the Class Members are domiciled; and (3) in the states in which the servers that provided services and communication links between Plaintiffs and the Class Members and Google.com and other websites with which they interacted were located.

385. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

386. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs and Class Members' personally

identifiable data in order to execute a scheme to defraud consumers by utilizing and profiting from the sale of their personally identifiable data, thereby depriving them of the value of their personally identifiable data.

387. Defendants have violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' computer systems and/or computer networks.

388. Defendants have violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' computer systems and/or computer networks.

389. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" is defined as "any set of computer instructions that are designed to ... record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

390. Defendants have violated California Penal Code § 502(b)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the Class Members and websites; specifically, a "cookie" that intercepts and gathers information concerning Plaintiffs' and the Class Members' interactions with certain websites, which information is then transmitted back to Google.

391. As a direct and proximate result of Defendant's unlawful conduct within the meaning of California Penal Code § 502, Defendant has caused loss to Plaintiffs and the Class Members in an amount to be proven at trial. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

392. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and declarative or other equitable relief.

393. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

COUNT THIRTEEN

STATUTORY LARCENY
California Penal Code §§ 484 and 496

394. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

395. Section 496(a) prohibits the obtaining of property "in any manner constituting theft."

396. Section 484 defines theft, and provides:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

397. Section 484 thus defines "theft" to include obtaining property by false pretense.

398. Defendant intentionally designed a program that would operate in a manner unbeknownst to Plaintiffs whose computers were thus deceived into providing PI to Defendant.

399. Defendant acted in a manner constituting theft and/or false pretense.

400. Defendant stole, took, and/or fraudulently appropriated Plaintiffs' PI without Plaintiffs' consent.

401. Defendant concealed, aided in the concealing, sold, and/or utilized Plaintiffs' PI that was obtained by Defendant for Defendant's commercial purposes and the financial benefit of Defendant.

402. Defendant knew that Plaintiffs' PI was stolen and/or obtained because Defendant designed the code that tracked Plaintiffs' PI and operated it in a manner that was concealed and/or withheld from Plaintiffs.

403. The reasonable and fair market value of the unlawfully obtain personal data can be determined in the marketplace.

COUNT FOURTEEN

VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*

404. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

405. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200.

406. Google is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

407. Google violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

408. Google's "unlawful" acts and practices include its violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the Stored Communications Act, 18 U.S.C §§ 2701, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Computer Fraud and Abuse Act, 18 U.S. C.§ 1030(g); the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; California Statutory Larceny, Cal. Penal Code §§ 484 and 496; and the Common Law Right of Privacy.

409. Google's conduct violated the spirit and letter of these laws, which protect property, economic and privacy interests and prohibit unauthorized disclosure and collection of private communications and personal information.

410. Google's "unfair" acts and practices include its violation of property, economic and privacy interests protected by the: Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the Stored Communications Act, 18 U.S.C §§ 2701, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Computer Fraud and Abuse Act, 18 U.S. C.§ 1030(g); the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; California Statutory Larceny, Cal. Penal Code §§ 484 and 496; and the Common Law Right of Privacy. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do so.

411. Google and Chrome promised Plaintiffs not to send their PI to Google even when Plaintiffs were Un-Synched. Plaintiffs thus had no reason to know and could not have anticipated

this intrusion into their privacy by the disclosure to Google of Plaintiffs' personal information. Google's conduct was immoral, unethical, oppressive, unscrupulous and substantially injurious to Plaintiffs. Further, Google's conduct narrowly benefitted its own business interests at the expense of Plaintiffs' fundamental privacy interests protected by the California Constitution and the common law.

412. Google's "fraudulent" acts or practices under the UCL include its misrepresentations and omissions assuring Plaintiffs that their PI would not be sent to Google while Un-Synched were intended to, were likely to, and did deceive reasonable consumers such as Plaintiffs. Google also misrepresented its privacy practices by disguising third-party tracking cookies as first-party tracking cookies, a practice already successfully challenged by the FTC in an earlier unrelated action. *United States v. Google, Inc*., 12-cv-4177-SI (N.D. Cal.). The information that Google misrepresented and concealed would be, and is, material to reasonable consumers, namely, that rather than not sharing the information at issue as represented, in fact that information was shared with Google.

413. Plaintiffs have suffered in jury-in-fact, including the loss of money and/or property as a result of Google's unfair, unlawful and/or deceptive practices, to wit, the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use and sale by Google. Plaintiffs have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.

414. Google's actions caused damage to and loss of Plaintiffs' property right to control the dissemination and use of their personal information and communications.

415. Google's misrepresentations and omissions—all which emanated from California—were material because they were likely to deceive reasonable consumers.

416. Google reaped unjust profits and revenues in violation of the UCL. This includes Google's profits and revenues from their targeted-advertising, improvements of Google's other products. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

417. Plaintiffs and class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Google's unfair, unlawful, and fraudulent business practices; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT FIFTEEN

PUNITIVE DAMAGES
Cal. Civ. Code § 3294

418. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

419. Google has an obligation not to intercept Plaintiffs' electronic communications without first obtaining consent, and this obligation exists by law independent of any contract with Plaintiffs.

420. California Civil Code Section 3294(a) allows Plaintiffs to recover additional damages "for the sake of example and by way of punishing the defendant" if the defendant is guilty of "oppression, fraud or malice."

421. Google intentionally caused injury to Plaintiffs and other Un-Synched Chrome Users by tracking their web use and collecting other PI without permission, and with a conscious disregard for their rights, making Google guilty of "malice" as defined by Section 3294(c)(1).

422. Google also intentionally misrepresented the privacy settings of Chrome, which was a material feature of the browser. Through Google's misrepresentation and deceit, Google deprived Plaintiffs and the other Un-Synched Chrome Users of property and privacy rights.

423. Google is liable for punitive damages in an amount to be determined at trial.

COUNT SIXTEEN

DECLARATORY RELIEF
28 U.S.C. § 2201(a)

424. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

425. An actual and justiciable controversy within the jurisdiction of this Court exists between the Plaintiffs and Google.

426. Plaintiffs seek an order declaring the rights of the parties arising out of the facts of this case, specifically an order declaring:

a. The Chrome Privacy Notice is a part of the contract between Chrome users and Google;

b. The data collected by Google from Chrome is Personal Information under the terms of the contract and under California law;

c. Google is in breach of the its contracts with Plaintiffs and Signed-Out Chrome Users by causing PI to be sent from Chrome to Google;

d. Google has violated the privacy rights of Plaintiffs and other Signed-Out Chrome Users by causing Chrome to collect and report users' PI to Google;

e. Plaintiffs have suffered privacy harm; and

f. Plaintiffs have suffered economic harm.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from installing cookies on its users' computers that could track the users' computer usage after logging out of Google or otherwise violating its policies with users;

D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant Plaintiffs such further relief as the Court deems appropriate.

IX. JURY TRIAL DEMAND

The Plaintiffs demand a trial by jury of all issues so triable.

Dated: July 27, 2020

BLEICHMAR FONTI & AULD LLP

By: *<u>/s/ Lesley Weaver</u>*
Lesley Weaver (Cal. Bar No. 191305)
Angelica M. Ornelas (Cal. Bar No. 285929)
Joshua D. Samra (Cal. Bar No. 313050)
555 12th Street, Suite 1600
Oakland, CA 994607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
aornelas@bfalaw.com
jsamra@bfalaw.com

SIMMONS HANLY CONROY LLC

By: *<u>/s/ Jay Barnes</u>*
Mitchell M. Breit (*pro hac vice* to be sought)
Jason 'Jay' Barnes (*pro hac vice* to be sought)
An Truong (*pro hac vice* to be sought)
Eric Johnson (*pro hac vice* to be sought)
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com

Attorneys for Plaintiffs

KAPLAN, FOX & KILSHEIMER LLP

By: *<u>/s/ David A. Straite</u>*
David A. Straite (*pro hac vice* to be sought)
Aaron L. Schwartz (*pro hac vice* to be sought)
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
dstraite@kaplanfox.com
aschwartz@kaplanfox.com

Laurence D. King (State Bar No. 206423)
Mario Choi (State Bar No. 243409)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com
mchoi@kaplanfox.com

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Lesley E. Weaver, attest that concurrence in the filing of this document has been obtained from the other signatories. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 27th day of July, 2020, at Oakland, California.

/s/ Lesley Weaver
Lesley E. Weaver